UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

LOCKHEED MARTIN TRANSPORTATION SECURITY SOLUTIONS, AN OPERATING UNIT OF LOCKHEED MARTIN CORPORATION,

Plaintiff,

-against-

MTA CAPITAL CONSTRUCTION COMPANY and METROPOLITAN TRANSPORTATION AUTHORITY,

Defendants.

No. 09 CV 4077 (PGG)(GWG)

DECLARATION OF
<u>HOWARD SAFIR</u>

TRAVELERS CASUALTY AND SURETY COMPANY OF AMERICA, FEDERAL INSURANCE COMPANY, and SAFECO INSURANCE COMPANY OF AMERICA,

Plaintiffs,

-against-

METROPOLITAN TRANSPORTATION AUTHORITY, MTA CAPITAL CONSTRUCTION COMPANY, NEW YORK CITY TRANSIT AUTHORITY, and LOCKHEED MARTIN CORPORATION,

Defendants.

No. 09 CV 6033 (PGG)(GWG)

TABLE OF CONTENTS

INITIAL EXPERT ANALYSIS

REBUTTAL TO THE AELLA / DESTEFANO REPORT

I, Howard Safir, declare under penalty of perjury that the foregoing is true and correct, pursuant to 28 USC § 1746(2):

1. The purpose of this declaration is to provide my opinion regarding the impact of the failure of Lockheed Martin Transportation Security Solutions ("Lockheed Martin" or "Lockheed") to deliver[1] the Integrated Electronic Security System/ Command, Control and Communications System of Systems (hereinafter the "Required System") as required by MTA Contract C-52038 (the "Contract"). Specifically, this declaration contains my opinion on the consequences of Lockheed Martin's failure to deliver the Required System on the safety of the people of New York City and surrounding areas, and MTA's assets and operations.

2. This declaration further responds to the Initial Expert Report Concerning Physical Security Technology Integration and Testing by Aella Consulting Group, Inc. (“ACG”) and Louis T. DeStefano, Inc. (“LTD”), dated June 21, 2011, prepared for Lockheed Martin (the “Aella/DeStefano Report”).

MY INITIAL EXPERT ANALYSIS

I. Introduction

3. It is my understanding that in its response to the RFP for Project C-52038, Lockheed Martin agreed to fulfill all of the contractual requirements for the Required System without exception and made numerous representations as to how it would effectively and efficiently deliver the Required System to help the MTA protect[2] its people, assets and

[1] For ease of use I will use the term "deliver" throughout this document to refer to Lockheed Martin's duties under the Contract to design, install, maintain, warrant, and support the Required System and provide the corresponding Concept of Operations, integration of Business Rules and operator training. It is important to note that the components are each critical and interrelated (i.e. you can't "install" the Required System if you fail to properly "design" it; you can't "maintain", "warrant" or "support" the Required System if you don't actually "install" it, etc.).

[2] For ease of use, I will use the term "protect" throughout this document to mean "prevent, deter, delay, detect, respond to and mitigate security incidents." These verbs and their related nouns (i.e. "prevention", "deterrence", "delay", "detection", "response" and "mitigation") are conceptually distinct, however, and at times correspond to

operations (collectively, "MTA Assets").

4. As shown through the project's testing record, which indicates that Lockheed never satisfied hundreds of important technical requirements, and based on numerous interviews I have conducted and observations I have made of the non-compliant system, it is clear to me that what Lockheed supplied to the MTA does not function or provide capabilities to security operations in a manner even reasonably close to what was required by the Contract.

5. I have reviewed and will opine on:

- Threats, vulnerabilities, and risks to MTA Assets from Security Incidents[3];
- The critical role and requirements of the Required System to reduce the likelihood and impact of Security Incidents;
- The substantive differences between the capabilities and operation of the Required System and the system that was supplied by Lockheed Martin and subsequently made partially functional by the MTA with the assistance of additional third-party vendors after the Contract was terminated (the "Lockheed System"[4]); and
- The significant additional casualties, repair costs, and down time to MTA Assets that may result from Security Incidents based on the MTA's hypothetical use of the Lockheed System as compared to the Required System.

II. Summary of Background and Qualifications

6. I am an almost 50 year veteran of law enforcement, emergency management, and the security industry. This includes service as the Police Commissioner of New York City, the

particular purposes, features or functions of the Required System. For example, a properly access-controlled door can both "prevent" and "deter" an incident by physically keeping an individual from a secured area, and an alarm that is triggered by breach of that door can help "detect", "respond" to and "mitigate" the security incident that may be related to the breach of that door.

[3] For ease of use, the term "Security Incidents" will include incidents that may cause casualties, injuries, property damage or interruption of MTA operations. These incidents may be caused by violent crime, terrorism, non-violent crime, accidents, acts of nature or other situations and circumstances that threaten MTA people, property and operations.

[4] At the time of Contract termination, the Lockheed System was not fully tested, installed, otherwise made operational or supported (i.e. training, maintenance, etc.). For purposes of this declaration, where I compare the operational use of the Lockheed System to the Required System, I make the counterfactual assumption that the Lockheed System was actually made operational, maintained and otherwise supported.

Fire Commissioner of New York City, the Associate Director for Operations at the United States Marshals Service, Assistant Director of the United States Drug Enforcement Administration and various management and board positions with private sector companies in the security industry. From my years of experience in these positions I am thoroughly familiar with the threats, vulnerabilities, and risks that face the New York City area and the various systems necessary to protect people and assets residing there from Security Incidents.

7. From my service as a government executive and my practice as a private security consultant and board member, I have significant direct experience with and knowledge of projects in which technical security systems have been successfully implemented to protect critical infrastructure and high volume, high profile facilities and systems.

8. My resume is attached as Exhibit A.

III. Summary of Findings & Conclusions

9. Unfortunately for the MTA and the millions of people who use its trains, buses, stations, bridges and tunnels on a daily basis, the Lockheed System does not even come close to meeting the requirements of Contract C-52038. It is missing critical capabilities. It lacks required features and modes of operation. In many respects it simply does not function at all. Moreover, the Lockheed System was only partially tested, nowhere fully installed by Lockheed and provided by Lockheed without critical training, maintenance and support to enable the MTA to gain utility from that system.

10. As detailed in this declaration, the Lockheed System fails to enable the MTA to prevent, deter, detect, respond to or mitigate the consequences of Security Incidents to the degree required by the Contract. Because of the deficiencies in the Lockheed System (detailed in Section VII, below), MTA is far more exposed to Security Incidents than it would have been if

Lockheed had delivered a contractually compliant system. Consequently, in the event serious Security Incidents occur, absent remedial measures to correct these deficiencies, more people would die, more property would be damaged and MTA operations would be interrupted for longer periods of time from Security Incidents, than if Lockheed had complied with the Contract. Correspondingly, the MTA's ability to protect MTA Assets from non-lethal Security incidents is also less than if Lockheed had complied with the Contract.

11. As a consequence of Lockheed's failure to deliver and install a system that complies with the contractual requirements, the MTA's Security Operators confront the following problems:[5]

- Lack of Awareness of Security Information: Security Operators are left unaware of certain alarms, alerts, notifications, and other critical data (hereinafter "Security Information");
- Unreliability of Security Information: Security Operators are unable to rely on the Security Information that they do receive;
- Lack of Understanding of Security Information: Security Operators lack required tools and training to sufficiently understand the Security Information that they do receive;
- Inability to Manage & Communicate Security Information: Security Operators lack required tools to help manage and communicate the Security Information that they do receive;
- Inflexibility: Security Operators are unable to enter and interact with Security Information in a flexible manner;
- Insecure Security Information: Security Operators are forced to use a system that does not properly secure Security Information; and
- Inefficiency: Security Operators are forced to use a system that is cumbersome and inefficient to operate.

[5] It is my understanding that Lockheed did not (and in some cases refused to and/or perhaps could not) deliver and implement certain functioning security devices (such as functioning cameras in the East River Tunnels and Grand Central Terminal). For purposes of comparing the features and functionality of the Non-Compliant Lockheed System versus the Required System, this section of the declaration will consider a hypothetical situation where such critical devices were properly installed.

12. Whether considering minor or catastrophic Security Incidents, the Lockheed System provides far less functionality and operational value than what was promised and contractually called for.

13. Put another way, the Lockheed System does not protect against Security Incidents as required by the Contract. With the Lockheed System, the MTA is in the unfortunate position of reactively responding to Security Incidents rather than taking the proactive and preventative approach that underpins the Required System (and that the MTA has every right to expect based on both the requirements of the Contract, commonly accepted security best practices and the reasonable expectation of the public). Even in this reactive position, the Lockheed System is unacceptably unreliable, slow, and disorganized in providing Security Operators with the critical Security Information they need to do their jobs in the effective manner required by the Contract.

14. My most conservative estimates indicate that Lockheed's failure to deliver the Required System has unnecessarily endangered thousands of lives, billions of dollars of property, and potentially adds months or years of service interruption to MTA customers from Security Incidents. This situation will continue until remedial measures necessary to reduce the risks that are the consequence of Lockheed's failure to deliver the Required System can be implemented.

IV. Facts and Data Considered for this Report

15. I considered the following sources of information in rendering my opinion:

1. My direct observations of the Lockheed System made at various times at the MTAPD Central C3 Center at Long Island City and the Long Island Rail Road regional C3 center at the Jamaica Station Complex;
2. The Contract;
3. The Project test records;

4. Interviews of the following MTA security professionals, MTA engineers, MTAPD officials and MTACC Project representatives (including engineers and project managers from Parsons Transportation Group/Parsons Brinkerhoff joint venture and Dnutch, Inc.):

   - Joseph Christen, MTACC
   - Ronald Pezik, MTACC
   - Kenneth Shields, URS
   - Terrence Fetters, Parsons
   - Shirsh Gupte, Parsons
   - William Morange, MTAPD
   - Ronald Masciana, MTAPD
   - Ernest Pucillo, MTAPD
   - William Coan, MTAPD
   - Ray McDermott, MTAPD
   - Leonard Viviano, MTAPD
   - Howard Reith, Dnutch
   - Robert Murphy, LIRR
   - John Highland, LIRR
   - Sean Ryan, MNR
   - April Panzer, MNR
   - Lisa Schreibman, NYCT
   - Staff at GuidePost Solutions

V. Threats and Vulnerabilities to the MTA from Security Incidents

A. Threats

16. The Required System was supposed to protect the MTA against Security Incidents from threats to the MTA including terrorism, other violent and non-violent criminal activity, accidents and weather-related incidents. As will be detailed in subsequent sections of this declaration, the Lockheed System provides far less protection against the threats described below than what was required by the Contract.

A.1. Terrorism

17. Since 1970 there have been over 1,700 terrorist incidents targeting mass transit around the world, including recent large scale attacks in London, Madrid, Paris, Moscow, and Tokyo that caused death and injury.[6] In these attacks, terrorists have used explosive devices, armed hijackings, chemical agents, shootings and sabotage.[7] I believe that future attacks on American transit systems are likely.

18. The MTA has been the target of several attempted terrorist attacks on its subways, commuter trains, buses, stations, and tunnels. These attempted attacks have included the planned use of explosive devices, armed hijackings and other means and methods to inflict casualties, injuries, economic damage and the interruption of transit operations.[8]

[6] Brian Jenkins and Bruce Butterworth, Explosives and Incendiaries Used in Terrorist Attacks on Public Surface Transportation: A Preliminary Empirical Examination, a publication of the Minetta Transportation Institute College of Business, San Jose State University, (March 2010), page 9.

[7] Ibid, 14.

[8] Other terrorist means and methods of concern to MTA Police include (but are not limited to) the potential dispersal of chemical and biological agents, the use of rolling stock as a weapon, and armed attack by one or more terrorists on indiscriminate targets (as in Mumbai). As a specific example of a terrorist action targeting MTA Assets, when I was Police Commissioner, the subway in Brooklyn was nearly attacked by three terrorists who were prepared to use nail scattering bombs to inflict casualties and injuries to MTA passengers. But for a tip that we received from a person directly involved with the terrorists, this plot may have remained undetected and otherwise not prevented. If the Required System had been installed, MTA would not have been as reliant on fortuitous tips about potential Security Incidents as it had been in the past.

19. Future terrorist attacks against the MTA are likely, based on the following factors:

- High occupancy of the MTA transit system;
- The criticality of MTA infrastructure to the local and national economy;
- The iconic status of many MTA stations and bridges and corresponding symbolic significance; and
- The location of MTA personnel and assets in New York City and the New York metropolitan area.

A.2. Other Violent and Non-Violent Criminal Activity. Accidents and Other Incidents

20. The MTAPD responded to 128,840 calls for service in 2010.[9]

21. The majority of these calls are generated by officers actively patrolling and inspecting the security of various MTA Assets. A high volume of these calls also comes from incidents reported by other MTA personnel and passengers as well as incidents generated by system alarms.

22. The nature of the MTAPD's calls for service ranges from violent and non-violent criminal activity, suspicious persons and conditions, accidents and other incidents that endanger people and operations.

23. Violent crime perpetrated on MTA Assets includes assault, robbery, rape and homicide. These incidents cause casualties, injuries and interruption of MTA operations. Accidents and unintended incidents that occur on MTA Assets include slips and falls, lost persons, power outages, service interruptions and potential issues related to MTA plant, property and equipment that may create a security condition for the MTA. Weather related incidents include the potential for flooding, crowding and service interruption from severe rainstorms (i.e. downed trees that cause track conditions), issues related to severe snowstorms and the possibility

[9] Source: MTAPD.

of earthquake or hurricane.

B. Vulnerabilities

24. Before considering appropriate mitigation measures, MTA Assets are generally vulnerable to Security Incidents based on easy public access to MTA Assets, the challenge of detecting human-based threats and incidents among very large and very dense crowds, and legacy security systems (and corresponding procedures) that were designed and implemented prior to the 9/11 terrorist attacks. These general vulnerabilities were intended to be addressed by the Required System in numerous features and functions of the Required System. As will be described in subsequent sections of this declaration, the Lockheed System leaves the MTA far more vulnerable to the various threats than it would have been had the Required System been delivered.

B.1. Vulnerabilities to Terrorism

25. The MTA is vulnerable to terrorist attack based on the nature of MTA Assets and operations, specifically:

- The relatively open-access nature of MTA Assets, including the ability to access the system to affect both major and minor assets from both central and remote locations;
- The large number of MTA users and the high density of users during a significant portion of the day (creating corresponding challenges of detecting terrorists planning, carrying or depositing explosives, chemicals, biological agents, guns, or other weapons in such a large and crowded transit environment);
- The low density of users during a significant portion of the day at non-patrolled stations (making it possible for a terrorist to access a remote station undetected by Security Operators or passengers);
- Stations, bridges, tunnels, rolling stock, and infrastructure built before 9/11 without emphasis on preventing or responding to terrorist attacks;
- Legacy operations and procedures that were developed before 9/11 without emphasis on preventing or responding to terrorist attacks; and

- Legacy physical security systems that were developed before 9/11 without emphasis on preventing or responding to terrorist attacks.

B.2. Vulnerabilities to Other Violent and Non-Violent Crime, Accidents and Other Incidents

26. The nature of the MTA's assets and operations also renders the MTA vulnerable to other violent and non-violent crime, accidents and weather-related incidents. As in the case of vulnerabilities to terrorism, the Required System was intended to address these vulnerabilities by improving the MTA's ability to protect against these incidents (see Sections VI and VII below).

27. The MTA is vulnerable to violent and non-violent criminal activity based on easy public access and a high density of users during a significant portion of the day and the low density of users during a significant portion of the day at non-patrolled stations (each dynamic creating difficulties in detecting and addressing criminal activity).

28. The MTA is generally vulnerable to the consequences of accidents and weather related incidents because many of its assets have a high density of people, many of whom are unfamiliar with MTA Assets and otherwise require significant direction, coordination and other assistance in the case of accidental/weather emergencies that can threaten life and safety.

C. The MTA's Post-9/11 Approach to Improving Security

29. To protect MTA Assets after 9/11, the MTA conceived and implemented a system-wide Security Program.[10] The Security Program included a series of seven task orders developed by outside security contractors for the MTA, including the task order that forms the basis of this lawsuit. The work performed under these task orders assessed the threats and vulnerabilities that confront the MTA, developed and implemented various projects and measures to address these risks, and ultimately aspired to protect MTA Assets through the

[10] Metropolitan Transportation Authority, *eM-1278 - Task Order's 1-7 : eomprehensive Threat Risk Vulnerabilitv Assessment Report*, September 15, 2004.

effective design, implementation, and operation of the Required System.

30. A key foundation to the Security Program is the Threat, Risk & Vulnerability Assessment ("TRV Assessment") that was completed in the fall of 2004, which categorized, measured, and addressed the likelihood and impact of terrorist incidents both before and after the implementation of appropriate mitigation measures.

31. The TRV Assessment applied a unified methodology of risk evaluation in which individual MTA stations, bridges, tunnels, infrastructure, and rolling stock were analyzed for the specific threats to each asset, the vulnerability of each asset, and the estimated casualties, property damage and impact to transit operations from specifically-considered terrorist incidents that may be carried out at one or more locations (hereinafter referred to as "Consequences of Security Incidents" or "Consequences"). These Consequences were considered both before and after the implementation of recommended security measures to protect against specific security threats at specific locations.

32. The recommended security measures include increased police patrols, structural hardening, other alterations to physical assets, and/or the implementation of electronic security systems and corresponding operational procedures.

33. Using this methodology enables the MTA to address logical issues of what threats at different locations can potentially do the most harm to MTA Assets and how to most effectively counter such threats and mitigate vulnerabilities. The specific methodology utilized by the MTA also enables it to estimate, for purposes of project prioritization and funding, how many casualties, how much property damage, and how much operational downtime it can avoid by the successful implementation of security projects at various specific locations.

34. The MTA Assets with the highest occupancies, highest property values, highest

levels of operational criticality, and greatest symbolic value, as well as the highest threat and vulnerability levels, are the MTA's highest priority security projects for funding and implementation.

35. The TVR Assessment resulted in the recommendation of security measures for "Phase I" projects such as Grand Central Station, Penn Station, Times Square, the Verrazano Narrows Bridge and the East River tunnels, as well as "Phase 2" stations, bridges and tunnels throughout the MTA System.[11]

36. To the extent that the MTA needed assistance in implementing its security projects, it issued Requests For Proposals ("RFP") for certain projects, which were bid out programmatically in a series of task orders, as noted above.

VI. The Goals of Project C-52038

A. Overview of Project C-52038

37. Project C-52038 (the "Project") was the task order to deliver the Required System. The Project is a critical component of the MTA's overall Security Program to reduce the Consequences of Security Incidents. The Project incorporated the electronic security system requirements of all of the Phase I sites described above as well as the Phase II projects referenced above, thereby protecting the most crowded, iconic, and vulnerable MTA Assets. The MTA is relying on successful implementation of the Project to protect against the Consequences of Security Incidents.

38. Project C-52038 required the contractor (Lockheed Martin) to

a) Deliver the Required System in conformance with approximately 17,000 contractual requirements;

b) Deliver corresponding business rules and a Concept of Operations ("ConOps")

[11] Including MTA Assets located in all five boroughs of New York City.

to operate the Required System;

c) Train MTA Security Operators to operate and maintain the Required System; and

d) Provide on-going maintenance, technical support, and training to support the Required System.

39. Strategically, the Required System specified in the Project was envisioned as a key tool in helping the MTA proactively protect against Security Incidents, going from a security system that was reactive and non-intelligent to one that would be proactive and intelligent. Before 9/11, the MTA had incomplete and disparate security systems. These non-integrated systems were deemed insufficient to protect against Security Incidents at single locations and, importantly, failed to "connect the dots" between multiple-location Security Incidents.

B. An Overview of the Required System

40. With the Project, the MTA sought to increase its levels of camera, access control and intrusion detection coverage, and to capture, organize, and communicate critical Security Information from both new and existing security devices within a single intelligent platform (i.e. the Required System).

41. The Required System specified appropriate decision support, communications, and security management tools necessary to protect MTA assets against Security Incidents. These security devices and security management tools are required to be integrated on a single platform and to function according to both inter-agency and intra-agency business rules (essentially operating rules within and between agencies that are required to be translated to system commands that direct the system to perform certain functions based on certain inputs

received in certain situations[12]).

42. The Required System was required to align with a Concept of Operations document that provides the strategic-level guidance of what the system is supposed to do and how it is supposed to be operated.

43. The basic architecture of the Required System is set forth in the Request for Proposals ("RFP") issued by the MTA Capital Construction Company on May 2, 2005, and is also apparent from the Required System's official name, the "IESS/C3 SoS":

- IESS - "Integrated Electronic Security System"

  The Required System was supposed to integrate Security Information from various subsystems located throughout the MTA and its agencies. These subsystems include camera systems, access control systems, intrusion detection systems, alarm systems and other security systems from various MTA Agencies[13] that observe occurrences in the physical world and convert the detection of such occurrence to Security Information to be received and managed by Security Operators (hereinafter the "Subsystems").

- C3 - "Command, Control and Communications"

  The Required System was supposed to provide centralized Command, Control, and Communications of Security Information at the MTA, at each MTA Agency on a central and regional basis.[14] This means that Security Operators can protect MTA Assets utilizing Security Information that they can comprehensively "command", "control" and "communicate" to other Security Operators both up and down the Chain of Command, both within MTA and outside of MTA as necessary (i.e. NYPD, FDNY, Department of Homeland Security, Department of Justice).

[12] For example, RQMT 1850("The Contractor shall provide a system, which funnels Alerts/Alarms upwards according to the business rules and the Decision Support Subsystem."); RQMT 1910 ("The Contractor shall ensure that a message is generated and published on the message bus when a security event (e.g., Incident or Emergency Situation) occurs, based upon the business rules."); RQMT 1912 ("The Contractor shall provide Incident Management/Decision Support that is automatically initiated once a security event message is received, based upon the appropriate business rules for the C3 Center."). See Also RQMTs 8, 1846, 2047, 1899, 1851, 1912, 1925, 1936, 1937, 1938, 1941, 1942, 1950, 1962, 1964, 1989, 2047.2, 2048, 2116, 2280, 2539, 2915, 3010, 3016, 17050 and 17060.

[13] MTA Agencies includes Metro North Commuter Railroad ("MNR"), Long Island Rail Road ("LIRR"), MTA Bridges & Tunnels ("B&T"), MTA Long Island Bus ("LIB") and MTA New York City Transit ("NYCT").

[14] 14 MTA Project C-52038 RFP. *Section 1AB2-Overview of the e3 eenters*, Pages 2-4. Lockheed Martin RFP Response, *Volume 1. Proposal Summarv. Solicitation No. e-52038. julv 22. 2005*, Page 11. Ibid, Volume II, Pages 4-10.

- SoS - "System of Systems"

  The Required System was specified so that it would manage both newly installed security devices and systems and legacy Subsystems from various MTA Agencies within a single system, and thus be a "System of Systems".

C. The Contractual Requirements of Project C-52038

44. The Contract specified a Required System to protect MTA Assets by providing comprehensive, accurate, timely, and efficiently-delivered Security Information to Security Operators both within and outside of the MTA. To accomplish this purpose, the Contract contained more than 17,000 requirements for the functionality, design, construction, business rules, Concept of Operations, implementation, testing, commissioning, training, maintenance, support, warranty, and system security of the Required System (the "Contractual Requirements").

45. As set forth in greater detail in Section VII, below, to achieve the goal of protecting the MTA's assets, the RFP's specifications required the contractor to demonstrate, among other things, that the system could meet the following overarching functional standards:

A. Security Operators and First Responders must be made fully aware of all alarms, alerts, notifications and critical data;

B. The information presented to Security Operators and First Responders must be reliable;

C. Security Operators and First Responders must have the tools and training to understand the information they receive;

D. Security Operators and First Responders must have the tools to manage the information they receive and be able to communicate that information to the right place and in a timely manner;

E. The Required System must not be cumbersome for Security Operators to operate, and it must be user friendly; and

F. Security Operators must have the ability to update critical information into the system.

46. The Required System was supposed to have the ability to protect sensitive information, both from those within the MTA who do not have authorization to access that data, and from those outside the MTA who wish to illegally obtain that data.

47. In addition, the RFP required that the system have training and maintenance modes. The required training mode was to ensure that current and future MTA personnel have the ability to quickly become competent in the use of the Required System without interfering with or compromising ongoing security operations.[15] The required maintenance mode would have allowed the system to be fixed as needed, and to be upgraded without downtime as technology developed.[16]

48. The above-referenced six overarching functionalities are fundamental to any operable security system and essential to satisfying three contractually mandated imperatives: "real time" decision-making, "situational awareness," and "interoperability" between MTA agencies and agencies outside the MTA. These imperatives include the contractually required concepts of "real time" decision-making (letters A-F above), "situational awareness" (letters A-D above) and interoperability between MTA and agencies outside the MTA (letter D above). Had

[15] See RQMT 2867 ("The Contractor shall provide a Command and Control System that provides a Training mode where fictitious events and corresponding scenarios are executed while maintaining normal security operations."); and RQMT 2868 ("The Contractor shall ensure it is possible to perform training/emergency response exercises while still providing the non-training features to authorized C2 Users who are not in Training Mode") and RQMT 2869 ("The Contractor shall provide a Command and Control System that specifies a level of training/emergency response so that no impact to normal operations of the MTA or the other agencies shall occur (e.g., commands to trains to bypass Penn Station are not sent and people are not prevented from entering the station).").

[16] See RQMT 2875 ("The Contractor shall provide the capability for an authorized C2 User to place the C3 Center into Maintenance Mode, when the C3 Center is being upgraded or repaired."). Regarding continuous operations during repair see RQMT 4010 ("The Contractor shall ensure any failed component is capable of repair and restart without disrupting the continuing operation of the C2 System.").

Lockheed satisfied the requirements of the Contract, the Required System would have operated in a manner consistent with these fundamental concepts, as defined below.

a. Real-Time Decision Making

49. I use the term "real-time" in this context to refer to the ability to receive and act on information immediately. Time is frequently of the essence in protecting MTA Assets against Security Incidents, and the ability to rapidly receive and manage Security Information can have great effect on the potential Consequences of Security Incidents. This need to gather Security Information in "real time" applies to both the preventative and response/mitigation aspects of the Required System. Shortcomings in "real-time" capacity can have an obvious and direct impact on security.

50. For example, if a critical element of Security Information is not available at a critical time to a Security Operator, a timely response cannot be initiated by that Security Operator. Likewise if a team of Security Operators in a chain of command has Security Information that is out of sync or inconsistent, crucial time will be lost as the team struggles to manually verify the Security Information rather than timely act upon it. If a security system does not provide reliable access to real-time Security Information then such a system is unacceptable to Security Operators where real-time security information is required.

51. Real-time decision-making is an integral component of the Required System. Detailed shortcomings in this area are highlighted in Section VII, below.

52. Further, Lockheed acknowledged in its RFP that real-time decision-making was part of the core of the Required System. For example, Lockheed Martin stated that its solution would provide an "operator-centric view [that] places the right information, in the right place, at the right time to assist the operator in making a decision about an event or group of events that

are taking place in real time."[17]

53. Lockheed also understood that its solution would offer a "variety of features and capabilities that can respond to threatening operational scenarios" including simultaneous events across two zones, a catastrophic event that damages a Regional C3 Center, and other specific security incidents.[18]

54. And Lockheed understood that the "Comprehensive ConOps and Business Rules" needed to be integrated into the system and corresponding Decision Support Systems so that the system would be "configured to support the C2 users at all levels of the MTA C3 operations."[19]

b. Situational Awareness Throughout MTA

55. As defined in the Project's Concept of Operations, Situational Awareness "is the ability to identify, process, and comprehend the critical elements of information about what is happening. More simply, it's knowing what is going on around you."[20]

56. To realize this concept, Security Information must not only be delivered in a timely manner, it must be sufficiently comprehensive and well-organized to be of the required value to the Security Operator. One way to analyze this concept is to ask whether Security Operators are sufficiently aware of a particular situation to effectively perform their individual

[17] LM RFP Response ("This operator-centric view places the right information, in the right place, at the right time to assist the operator in making a decision about an event or group of events that are taking place in real time."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 4.

[18] LM RFP Response ("Our design provides a variety of features and capabilities that can respond to threatening operational scenarios, such as those shown in Table 1.1-1."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 4.

[19] LM RFP Response ("A comprehensive set of constructs representing the ConOps and Business Rules will be integrated into the IESS/C3 solution capabilities to assist C2 operators in responding to security events."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 87.

[20] MTA Concept of Operations Definition ("Situational Awareness- is the ability to identify, process, and comprehend the critical elements of information about what is happening. More simply, it's knowing what is going on around you."), *MTA IESS & e3 Svstem of Svstems eoncept of Operations* (ConOps), Parsons Transportation Group, Revised by Lockheed Martin Company, February 6, 2006, Page 79.

and collective duties to protect an MTA Asset against a Security Incident.

57. As the MTA has disparate assets managed by different MTA Agencies, the ability of Security Operators to receive, manage and communicate Security Information both within and across MTA Agencies is essential in order to achieve the required Situational Awareness.

58. Toward this end, the RFP specifications called for, among other things, capability referred to as a "Common Operational Picture." This feature enables Security Operators within an agency, or across different agencies, locations or departments to have access to Security Information on a single system using the same display of relevant information.[21]

59. Lockheed, in its Proposal, understood that Situational Awareness was integral to the Required System. For example, Lockheed stated that its solution would enable the operator "to intelligently reach into any available Monitored Location providing the necessary situational awareness to manage events as they develop."[22] Further, Lockheed understood that it would have to provide a "Common Operational Picture" configured for each Agency, thereby allowing decision-makers to have access to the necessary and appropriate data as the situation demanded in order to formulate optimal responses.[23] Detailed failings in this area in the Lockheed System

[21] MTA Concept of Operations Definition ("The Common Operational Picture (COP) provides the latest plan and status information, CCTV displays, GIS displays and can be customized by each of the users to present information that is important to them and in a manner that is applicable to their operation. The COP will provide each user with the overall status of the MTA across all of the Agencies to support the early identification of problems that may impact their security or operations."), *MTA IESS & e3 Svstem of Svstems eoncept of Operations*, Parsons Transportation Group, Revised by Lockheed Martin Company, February 6, 2006, Page 19.MTA RFP ("The Contractor shall, as part of the design phase, work with the MTA and each Agency to define what pertinent information to display on the COP associated with specific alarm information or detected threats. The Contractor shall provide a Common Operational Picture with a capability to use voice, video, data, imagery and graphics to present pertinent information on the COP."), *Project e-52038 RFP. Section 1AB4-eommand and eontrol (e2) Svstem*, Page 29-31; 1AB4, 4.5.

[22] LM RFP Response ("The C2 display on an individual operator's workstation will allow an authorized user to intelligently reach into any available Monitored Location providing the necessary situational awareness to manage events as they develop."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 12.

[23] LM RFP Response ("The COP is configured for each Agency, thereby allowing decision makers to have access to the necessary and appropriate data as the situation demands in order to formulate the optimal response."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 36.

are identified below in Section VII.

c. Interoperabilitv Between MTA Agencies and Agencies Outside the MTA

60. Protection of MTA Assets is the job of Security Operators not just within various MTA Agencies, but crucially, outside of MTA as well.

61. The Required System was supposed to make various Subsystems utilized by both MTA Agencies and agencies outside the MTA, such as the NYPD and FDNY, "interoperable" so that both the preventative and responsive aspects of protecting MTA Assets against Security Incidents could be properly facilitated.

62. Especially where various agencies and multiple chains of command are involved, the efficiency, security, comprehensiveness and format by which Security Information is communicated are critical to the protection of MTA Assets.

63. Lockheed Martin understood that, as required by the Contract, the system would need to interface with a "multitude of metropolitan, state, and federal organizations" including federal, state and local law enforcement and first responders.[24] Lockheed specifically stated that it would provide interoperable voice communications[25] and further, that it would provide the ability to share live video across the police community.[26] Detailed failings in this area in the Lockheed System are identified in Section VII, below.

[24] LM RFP Response ("As indicated in the context diagram in Figure 1.0-2, there is a multitude of metropolitan, state, and federal organizations that must interface with the IESS/C3 system. The proposed architecture supports implementation of the variety of requested interfaces with these external agencies and affiliated organizations, including formatted message data, e-mails, faxes, and voice communication."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 3.

[25] LM RFP Response ("The C3 Communications System provides mission-critical voice and data services for the MTA Police. The communications equipment integrates with the various agencies to support a system-wide interoperable solution."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 44.

[26] LM RFP Response ("Our video services solution allows live video inputs from related agencies, Smart Sites, television feeds, and conferencing systems to be shared on an as needed, secure basis, in addition to allowing the selection and transmission of recorded video."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 46.

VII. The Substantive Differences Between the Required System and the Lockheed System

64. I have grouped the many failures in the Lockheed System into seven major functional categories, as seen from the Security Operator's perspective, identified in subsection A and B below. Each of these major functional categories is, in turn, divided into more specific categories of functionality, each of which contains requirements taken directly from the Contract documents, none of which passed the tests that Lockheed performed to determine whether the functionality existed in the system. The failure of the Lockheed System to meet each subgroup requirement is documented by the test records and is further supported by my own observations.

65. The Lockheed System falls far short of satisfying the contractual requirements for these major functional areas. As delineated below, the Lockheed System (i) fails to make Security Operators and First Responders fully aware of all alarms, alerts, notifications and critical data; (ii) it does not ensure that the Security Operators receive reliable information; (iii) it does not provide the tools and training so that the Security Operators have the requisite level of understanding of the information they receive or (iv) the ability to manage and communicate that information, (v) and to do so easily and conveniently; and (vi) it does not allow Security Operators to update critical information in the system. The Lockheed System also does not allow the required protections for sensitive information.

66. These failures result in the Lockheed System's overall failure to provide MTA with the fundamental features called for by the Required System and correspondingly the Lockheed System does not support real time decision-making, situational awareness, and interoperability between MTA agencies and outside agencies as required.

67. As a result of Lockheed's failures, summarized above and described below, and the consequential failures to provide a system with the three fundamental features referenced in

this paragraph (described in Section VI, above), the MTA is left with a system that makes it far more difficult to effectively protect against Security Incidents than would be the case if Lockheed had delivered what was contractually required and what it promised to do.

A. Problems with the Lockheed System from the Security Operator's Perspective

A.1. Lack of Awareness: Security Operators and First Responders Will Miss Alarms, Alerts, Notifications and Other Critical Security Information

68. A key foundation of the Required System is for Security Operators to be aware as quickly as possible that an alarm, alert or notification has occurred. At the most basic level, for this to happen at all, the Subsystems must be functioning and Security Operators must receive the required Security Information. To Protect MTA Assets, the Contract required that certain Security Information be automatically generated and transmitted to Security Operators within and across MTA Agencies.

69. In agreeing to meet 100% of the Contractual Requirements, and in specific statements made in their RFP response, Lockheed Martin agreed to deliver a security system that would seamlessly transmit Security Information to Security Operators.

70. The unsatisfied Contractual Requirements and examples cited and described in this section illustrate how the Lockheed System's shortcomings in detecting and communicating Security Information reduce the MTA's ability to effectively protect MTA Assets against Security Incidents as required.

i. Lack of Diagnostic Tools to Know if Devices in the Field Are Functioning

71. The Lockheed System lacks required tools to allow Security Operators to know if devices in the field are functioning at all[27] and to allow Security Operators to make remote

[27] See RQMT14837 ("The system shall detect and display an alarm if video from a particular camera is lost."), and RQMT14781 ("The system shall be capable of raising an alarm if video becomes undetectable , or if an image luminance falls below a configurable threshold."); see also RQMTS 2101, 3523, 3637, 14838, 14840.1, 15477 ("The

adjustments to the devices so they can obtain useable Security Information from such devices.[28]

72. For example, the Lockheed System would not alert a C3 center if a camera (or group of cameras) was not working to protect a critical MTA Asset. Likewise, if conditions change (such as changes in light levels or another condition) so as to make an otherwise technically functioning camera unable to transmit useable images to the command center, the Lockheed System would not report this condition change to the C3 center, nor does the Lockheed System provide required tools that allow the Security Operator to remotely adjust a camera's settings to accommodate the condition change.

73. This lack of functionality will cause Security Operators to receive no practical use from certain security cameras or alarms, or will place them in a situation where Security Operators are not made aware of situations where security devices are either wholly or partially not functioning.

ii. Non-Integration of Field Security Devices to the Command Centers

74. The Lockheed System does not integrate Security Information from cameras, access control, motion detection and other field devices into a Graphical User Interface (i.e. a window on a computer screen that a human Security Operator can effectively monitor).[29]

contractor shall provide sensors and security devices capable of being monitored by the system and their condition to be displayed to alert the operator.")

[28] See RQMT3043.2 ("*The eontractor shall provide a eommand and eontrol Svstem that provides a capabilitv for authorized e2 Users to add!delete and modifv the information that is obtained from the external svstems*.");see also RQMT 14592 ("The intercom shall be capable of being tested by an automatic remote diagnostic system for all of its functions."), RQMT 14593 ("The system shall be capable of reporting its status.") RQMT 14782 ("The frame rate, resolution and bandwidth shall be individually adjustable for each camera."), RQMT 14783, RQMT 14784, RQMT 14787.

[29] See RQMT 2137 ("The Contractor shall furnish a CCTV system that has an open API to include third-party integration with other systems like the access control and field devices.″), RQMT14652 ("The functions of the monitored locations and smart sites as described in this specification shall be accomplished through the Video Surveillance System and through the integration of the Video Surveillance System with the access control system.″), RQMT14825 ("Alarms from the Video Surveillance System, shall be integrated with the facility's access control system.″), RQMT14914 ("When a camera's field of view covers a security detection device or intercom unit, the

75. For example, if a terrorist seeking to sabotage a track physically breaches multiple areas, and such breach is detected in one instance by a video camera and the other instance by a motion detector, rather than integrating this Security Information, the Lockheed System sends the alarms generated from these two Subsystems to two separate and unrelated non-integrated systems that are virtually impossible for a human security operator to correlate, as required by the Contract.

76. As a result, the MTA would have to rely on its Security Operators to somehow perform a virtually impossible correlation between related events that were separately reported by the Lockheed System. Consequently, with the Lockheed System, a Security Incident will be able to develop undetected for a longer period of time (and thus may result in more damage to persons and property) before the appropriate response is undertaken than if the MTA had the Required System.

iii. Lack of Automated Alarms, Alerts and Notifications

77. The Lockheed System fails to incorporate various automated alarms, alerts, and notifications to supplement and support live monitoring of multiple programs and/or screens as required by the Contract.[30]

78. For example, if a critical area is breached and this breach is picked up by a

system shall be capable of displaying the appropriate video from that camera when the security detection device or intercom unit is activated."), RQMT1869.2 ("The Contractor shall provide database servers configured, where compatible with the applications, to allow the maximum flexibility possible for database interconnectivity and the seamless exchange of data with software applications."); see also RQMTS 2143, 3803.1, 3296, 3628, 15392, 14495, 14515, 14514, 16766.

[30] See RQMT14591 ("*Operation of the intercom svstem shall be integrated with the video svstem so that operation of an intercom unit shall cause the appropriate camera covering that unit to displav video on the assigned monitor at the monitoring location."*), RQMT2119 ("*The eontractor shall provide a eommand and eontrol Svstem that generates an alarm message based upon the analvsis of alarm information that detects aggregated alarms or inferred alarms."*), RQMT14847 ("*The Video Surveillance Svstem shall be fullv integrated with an intelligent video monitoring subsvstem."*), RQMT3709 ("*The eontractor shall provide the abilitv to send!receive eeTV video images to!from NYPD"*); see alsoRQMTS 2109.1, 2566, 2567, 2568, 2578, 3802.2, 3343, 3344, 3345, 3390, 3420, 3421, 3433, 3434, 3439, 3441, 3442, 3443, 3447, 3448, 3449, 3451, 15476, 15477, 15478, 15479, 14490, 15476.

security device on the intrusion detection subsystem, the Required System would generate an automated alarm to a defined user group of Security Operators. The Required System would also send corresponding video to the MTA command centers and to the New York Police Department ("NYPD") as per defined protocols and procedures. This automated alarm would substantially reduce or eliminate the necessity for Security Operators to manually monitor certain screens (thus enabling them to monitor elsewhere and otherwise do their job as effectively and efficiently as possible). The Lockheed System does not provide this functionality.

79. This failure seriously impairs the ability of the MTA to timely and adequately respond to the specific incidents that are not automatically reported, and limits the overall effectiveness of the Security Operator and time in which he/she has to carry out other duties.

iv. Inability to Automatically Disseminate Alarms, Alerts, and Notifications to Security Operators, First Responders and Other Responsible Parties

80. The Lockheed System lacks tools to automatically disseminate certain Security Information to defined user groups.[31]

81. For example, if a terrorist enters a prohibited LIRR track area leading into Penn Station, the intrusion detection system in the Required System is supposed to automatically notify multiple specific agency contacts (from a list that the Required System would allow the MTA to update with current and accurate information) within Long Island Railroad and the MTA Police and provide each of the recipients with key data related to the alarm (such as the time of occurrence or the specific location). The Lockheed System does not include this functionality.

[31] See RQMT2118 ("The Contractor shall provide the capability for an authorized C2 User to initiate a re-analysis based upon the new security alarm information."), RQMT 2128.1 ("The Contractor shall provide a Command and Control System that facilitates intrusion detection notification that identifies the appropriate Agency to notify, the Agency personnel to contact and provides any alarm information concerning the potential intruder, the time of the intrusion and the location of that intrusion.″); see also RQMTS 2553, 2558.2, 2559, 16446.

82. As a result, compared to the Required System, certain key individuals will not be notified of critical security incidents in a timely fashion and key decision-making and appropriate incident response will be delayed (or otherwise less effective).

v. Lack of Business Rules and Decision Support Tools to Communicate Alarms, Alerts, and Notifications

83. The Lockheed System lacks business rules, decision support tools, and communications tools to help an individual Security Operator share critical Security Information.[32]

84. For example, if a Security Operator in the Metro North Regional C3 Center is notified of a breach of a secure area on the upper level and lower level tracks of Grand Central, the Required System's software should automatically indicate to that operator what situation the breach may represent, and also provide the Security Operator with a set of instructions as to what to do and who to contact within the MTA.

85. In its response to the RFP, Lockheed Martin stated that "[a] comprehensive set of constructs representing the ConOps and Business Rules [would] be integrated into the IESS/C3 solution capabilities to assist C2 operators in responding to security events ."[33]

86. The Lockheed System does not include the above described functionality, which means that, compared to the Required System, the MTA must rely upon its Security Operators to

[32] See RQMT 1850 ("The Contractor shall provide a system, which funnels Alerts/Alarms upwards according to the business rules and the Decision Support Subsystem.*"). RQMT 2047.1 ("The Contractor shall provide a system that is capable to create, aggregate and forward alarm indicators based upon pre-defined business rules and access control."), RQMT2117 ("The Contractor shall provide a Command and Control System that performs analysis of alarm information to detect threats, based upon the defined business rules."), RQMT 2520.1 ("The Contractor shall provide Alarm Management that manages Alarm, Alert and Notification messages initiated by the Command and Control System, using the Publish/Subscribe mechanism."); see also RQMTS 2529, 2539.2, 2541.2, 2542, 2543.2, 3781.2, 3784, 3594, 14845.

[33] LM RFP Response ("A comprehensive set of constructs representing the ConOps and Business Rules will be integrated into the IESS/C3 solution capabilities to assist C2 operators in responding to security events."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 87.

make decisions without the benefit of required tools and knowledge, and for certain incidents, to manually correlate information that they do not have and/or otherwise cannot manually correlate.

87. For example, in the scenario described above, an individual MTA security operator (or multiple security operators on shift) may fail to make the important correlation between breaches on separate tracks at separate times that may, in reality, be part of the same Security Incident; if they do correlate the breaches and seek to take action based on that correlation, they will do so without the required support from the Lockheed System.

88. Further, as with Lockheed's failure to provide the automatic notifications required by the Contract, the lack of business rules and decision support tools means that Security Operators may notify the wrong people of incidents or take an unnecessarily long time manually looking up current contact information which should be automatically provided by the system.

vi. Inability to Store, Archive and Play Back Critical System Information

89. The Lockheed System lacks the capability and functionality to properly store, archive, and play back critical alarms, alerts, notifications and otherwise retrieve critical data in various formats.[34]

90. For example, if a terrorist leaves a bomb or device containing harmful gas in a trash can in Penn Station and law enforcement needs to quickly review video of that incident and video from other cameras throughout the MTA system to determine if additional devices were

[34] See RQMT 2132.1 ("The Contractor shall provide a Command and Control System that provides all functionalities through User Interface for local and remote locations, via the network, setup and control of parameters governing the recording, and playback of CCTV images processed by all DVRDs."). and RQMT 2785 ("The Contractor shall provide, from historical data, Information Playback capability that recreates the conditions and user interactions during a specified time period. **A playback workstation shall be capable of displaying data and information from a selected time period of an event that occurred in the past. (no dedicated workstations exist for playback - any C3 workstation may be used to play back information).),** RQMT 2786 ("The Contractor shall provide the same display formats for Playback as for actual C3 operations, except that a clear, distinguishing attribute (e.g., a combination of text with a uniquely colored border) should be provided to distinguish displays presented during Playback from those presented of live video during actual C3 operations".). and RQMT 2788.3 ("The Contractor shall provide an Information Playback capability that retrieves video from the user-selected date and time period, from historical archives."); see also RQMTS 2545.2, 2546.2, 2547.2, 2615.2.

left in other stations, the Lockheed System would not be able to rapidly perform such a function.

91. This lack of functionality means that Security Operators will not have access to critical information to know what happened (or may still be happening) in a related incident as required.

vii. Inability to Conduct Post-Event Forensics

92. The Lockheed System lacks the promised capability to capture historical records and changes made during an event[35] and to provide post-event forensic data for audit, review and investigations.[36]

93. For example, if a suicide bomber enters the subway system in Flushing and travels via subway to Times Square, where he detonates a bomb, the MTA will be unable to determine to the extent required what information was received by its Security Operators from the various video, alarm, and explosive detection systems when it later attempts to review the incident. Nor would the required details of the Security Operators' communications or actions to address the incident be available as required, post-event.

94. The Lockheed System's inability to provide this critical information in the post-event forensic context means that the MTA is far less able to teach its Security Operators how to better utilize the system and its corresponding procedures, and it will not have all of the critical information necessary to make essential improvements to the system or to help address potential public communications, legal, or other consequences regarding its response to incidents.

[35] See RQMT 2090.1 ("The Contractor shall provide a Resource Log or a historical record of all changes to asset and resource information, all Response Plans, changes made to plans, all events entered and all alarms and messages displayed to all C2 Users. "), and RQMTS 2506, 14595, 2023, 2037, 2038.

[36] See RQMT 2455 ("The Contractor shall provide a means that allows user changes to pre-specified automatically entered fields but shall log the automatically entered value, along with the user-entered value for an audit trail. "). and RQMT 2029 ("The Contractor shall provide Post-Event Forensic Investigation that collects performance data for scenarios to run as training exercises or as real life responses to emergency situations. "); see also RQMTS 2465, 2465.1, 2465.2, 2466, 2467.1, 2778.

viii. Inability to Communicate Between C3 Centers

95. The Lockheed System lacks the ability to effectively and quickly communicate certain Security Information to individual C3 centers.[37]

96. For example, the Required System specifies the ability to directly signal C3 centers by pushing a single button. In the Lockheed System, this function does not work and thus communications take more time.

97. Additionally, the Lockheed System completely lacks the required "Emergency Mode,"[38] and thus a Security Operator cannot put the system in such a mode and automatically alert the necessary C3 center personnel as to one or more Security Incidents (and, importantly, the Potential Consequences of such Security Incidents) as required. Instead, the Security Operator must manually notify each Security Operator at each C3 center of an emergency.

A.2. Security Operators and First Responders Will Be Unable to Rely Upon Security Information that is Actually Received

98. Security Operators must be able to rely on the Security Information that they do receive. At the most basic level, Security Operators need to know the source of the Security Information and whether or not any such user-entered Security Information has been validated for its completeness and accuracy.

99. In agreeing to meet 100% of the Contractual Requirements, and in specific

[37] See RQMT 1899 ("The Contractor shall provide a Command and Control System with all of the C2 functionality at all of the C3 Centers, but the functionality at each C3 Center is data and business rule driven.*:).* RQMT 1909 ("The system shall be capable of allowing an authorized C2 User to initiate a change of Mode of Operation to Emergency Mode when a security event (e.g., Incident or Emergency Situation) occurs, only when the C3 Center is in Operational status and in Normal Mode*".).* and RQMT 1913 ("The Contractor shall provide the capability for an authorized C2 User to initiate a change of the Mode of Operation to Normal Mode when the security event is closed, only when the C3 Center *is in* Operational status (the C3 Center is operational - running and functioning as a C3 Center) and in Emergency Mode."); see also RQMTS 2049.2, 2526.2, 3045, 3111, 14590.

[38] See RQMT 1902 ("The Contractor shall provide a system that, when in Emergency Mode, provides all the capability of Normal Mode and adds functionality to assess security incidents or potential security incidents that might adversely affect MTA operations, employees, or passengers and provide Incident Management/Decision Support capability.").

statements made in their RFP response, Lockheed Martin agreed to deliver a security system that would inform Security Operators of the required details about the source of Security Information and provide tools to validate user-entered Security Information.[39]

100. The unsatisfied contractual requirements and examples cited and described in this section illustrate how the Lockheed System's shortcomings in ensuring the reliability of critical security information impairs the efforts of the MTA to effectively protect MTA Assets against Security Incidents as required.

i. Inability to Provide Critical Information About Alarms, Alerts, and Notifications

101. Despite the specifications of the Contract, the Lockheed System does not provide Security Operators with the source, time, and nature of certain Security Information.[40] Accordingly, a Security Operator will not possess critical data about certain Security Information that may have been entered into the system by him/herself or another operator.

102. For example, when an access control alarm on a door is triggered, the Lockheed System does not provide descriptive information about the location of a door (or the criticality of where the door leads) but only supplies a reference number, which the recipient of the alarm

[39] MTA RFP ("The Contractor shall provide a Command and Control System where input data is checked at the source of data entry, in order to ensure prompt and proper correction of the data by the person entering the data."), *Project e52038 RFP. Section 1AB4-eommand and eontrol (e2) Svstem*, Page 41.LM RFP Response ("The Lockheed Martin/ARINC Team takes NO contract exceptions. Our proposed offering is 100% compliant with MTA Capital Construction Company's Request for Proposal."), *Volume 1. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 19.

[40] See RQMT 2450 ("The Contractor shall ensure data automatically entered by Alarm Management includes, but is not limited to date, time, a marker indicating whether the operational event has been automatically or manually generated, person entering the event, the alarm that precipitated the automatic creation of the event, the location involved in the event, and a serialized operational event number."), RQMT 2163.2 ("The Contractor shall provide a Command and Control System that provides authorized C2 Users with the capability to choose to view any or all indicators, that they are authorized to view by geographical selection."), RQMT 2164.3 ("The Contractor shall provide a Command and Control System that provides authorized C2 Users with the capability to choose to view any or all indicators, that they are authorized to view by individual or group selection.″), and RQMT 2281.3 ("The Contractor shall provide a Command and Control System where input data is checked in order to ensure prompt and proper correction of the data entered."); see also RQMTS 2030, 2032, 2033, 2034, 2035, 2056, 2590.

must decode. This significantly slows response time.

103. For another example, if a Security Operator in the Local C3 Center at Jamaica, Queens generates a manual alert based on a passenger's report of the suspicious activities of a specifically-described man (a "See Something, Say Something" report), a shift supervisor arriving on the next shift will be unable to use the Lockheed System to understand when, why or how such an alert was generated.

104. Moreover, the complete absence of the contractually-required Emergency Mode and Normal Mode makes it so the alarm cannot be properly put in context as required (i.e. the system does not indicate that this incident generated an "Emergency Mode" operation).

ii. Inability to Validate-User-Entered Data

105. The Lockheed System lacks tools to validate user-entered data.[41]

106. For example, if a Security Operator inaccurately or incompletely enters the date, time, or location of suspicious activities (i.e. if the street address does not match the borough-entered field or the date entered field is accidentally typed as a future date), the Lockheed System would not correct these data entry errors or alert any Security Operators to them.

107. Without such validation tools, the MTA is overly reliant on the accuracy of each operator in entering information, and in the case where a Security Operator enters inaccurate information, the MTA is more likely to proceed with an inappropriate and/or ineffective response to Security Incidents.

108. This also negatively impacts MTA's ability to do forensic analysis of Security

[41] See RQMT 2281.1 ("The Contractor shall provide a Command and Control System where all user-entered data is validated for reasonableness of content."), and RQMT 2282.1 ("The Contractor shall provide a Command and Control System where all entered data is validated.″), and RQMT 2283.1 ("The Contractor shall provide a Command and Control System where input data is checked at the time of entry in order to ensure prompt and proper correction of the data by the person entering it."), and RQMT 2005 ("The Contractor shall provide Execution Management that prompts authorized C2 Users for missing information, allowing them to enter complete or partial information in response."); see also RQMTS 2300, 2301, 2626, 2938.2, 2942.2.

Incidents. Because of the lack of data validation in operator-entered information, "Penn Station" could be entered in system information as "Penn Station," but also as "PS," or "PSNY," or any other variation an operator may think of. This also makes it difficult for MTA to aggregate and search data that is entered by operators.

A.3. Security Operators and First Responders Are Not Supplied the Tools and Training to Understand the Limited Security Information Received

109. Security Operators need to understand Security Information within the context of a potential or occurring Security Incident. A basic foundation to such understanding is proper Security Operator training on the Required System. The Required System also specified critical analysis & intelligence tools to help Security Operators understand Security Incidents.

110. In agreeing to meet 100% of the Contractual Requirements, and in specific statements made in their RFP response, Lockheed Martin agreed to deliver a security system that would help Security Operators understand Security Information.[42]

111. The unsatisfied contractual requirements and examples cited and described in this section illustrate how the Lockheed System's shortcomings in analyzing critical security information make it much more difficult for the MTA to effectively protect MTA Assets against Security Incidents than would be the case if Lockheed delivered and installed the Required System.

i. Insufficient System Training Functions

112. The Lockheed System lacks key training functions, including a separate Training

[42] MTA RFP ("The Contractor shall provide a Summary Representation capability to represent asset and resources in representations best suited for quick and easy understanding," "The Contractor shall provide displays that are clear, understandable and have a minimum of extraneous information."), *Project e-52038 RFP. Section 1AB4-eommand and eontrol (e2) Svstem*, Page 39, 41. LM RFP Response ("Because the quantity and variety of information collected via multiple-system components can be intrinsically difficult for the C2 operator to mentally collate and understand, our geographical-based representation of resources and information provides an ideal mechanism to couple real-time situational data with event-response guidance, predicated on Agency-generated business rules."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 34.

Mode and specific simulator and scenario-based training functions required by the Contract.[43] This means that the Lockheed System does not enable MTA to train its C3 Center staff for potential scenarios.

113. Without these critical training functions (standing alone and in combination with the manifold other system shortcomings described herein), Security Operators are less prepared and capable of executing an effective response when addressing Security Incidents.

114. The lack of Training Mode also means it is much more difficult to train new Security Operators, who must be trained on the live Lockheed System, rather than in a safe practice environment as called for in the Required System specifications.

ii. Lack of Analysis and Intelligence Tools

115. The Lockheed System lacks the critical real-time analysis and artificial intelligence tools of the Required System.[44] This lack of functionality means that the MTA's

[43] See RQMT 2878 ("The Contractor shall provide a Simulator that supports the simulation of all conditions and functions supported by the IESS."), and RQMT 2884 ("The Contractor shall provide a Simulator that simulates the normal and failure operation of the security devices within the system by using programmed simulation data and/or simulated alarm inputs."), and RQMT 2886 ("The Contractor shall provide a Simulator that simulates the operation and functionality of any external device or system, and manual inputs from authorized C2 User (e.g., a Trainer injecting failures into the system)."), and RQMT 2889 ("The Contractor shall provide a Simulator that is capable of generating simulated data for all external systems."*)*; *see also* RQMTS 2877, 2878, 2877, 2885, 2887, 2888, 2890, 2891, 2893, 2895, 2902, 2903, 2906, 2907, 2908, 2909, 2910, 2911, 2912, 2916, 2918, 2919, 2924.1, 2925.1, 2929, 2930, 2932, 2933, 14608.

[44] See RQMT 2138 ("The Contractor shall provide a Command and Control System that provides for rapid evaluation of available information to quickly determine situations requiring attention (e.g., emergencies, terrorist attacks, and life threatening incidents."), RQMT 2117 ("The Contractor shall provide a Command and Control System that performs analysis of alarm information to detect threats, based upon the defined business rules."),RQMT 2119 ("The Contractor shall provide a Command and Control System that generates an alarm message based upon the analysis of alarm information that detects aggregated alarms or inferred alarms."), RQMT 40.1 ("Computer analytics shall also be deployed for artificial intelligence that will generate alarms for anomalies such as motion detection."), and RQMT 2115.2 ("The Contractor shall provide a Command and Control System that logs all alarm analysis information, including raw data used to determine the alarm."); see also RQMTS 2103, 14848, 14850, 14853.2, 14855.2, 14858, 14859, 14860, 14861, 14864, 16372. Also, please note LM RFP Response, Proposal Volume 1, Page 12 ("The Core HIViewTM COTS products were selected based on their rich feature and function sets; scalability; ability to be easily configured to unique business rules; suite of interface protocols; and decision analysis and support tools."); Volume II, Page 4 ("Our design applies decision-support tools to suggest or direct operator actions based on operational policies that will be captured collaboratively with MTA Capital Construction Company (CCC) as Agency-specific business rules within the system, described later in Section 3.3 as

response to a Security Incident using the Lockheed System would be overly reliant on the human security operator to analyze alarms, relate such alarms to potential incidents, and make appropriate decisions to address such incidents.

116. For example, if there are multiple security incidents at rail yards at three outlying stations on the Metro North system over a given period of time, this may indicate that terrorists are seeking to breach the integrity of a Metro North commuter train(s) to subsequently derail or attack such train(s) or explode such train(s) at a crowded Metro North station such as Grand Central Station.

117. It is important to note that while the Contract does not require the system to automatically make the specific conclusion of this hypothetical example per se (i.e. breaches of commuter trains on outlying rail yards = a possible attack on a crowded central station), the Contract specifies that alarms must be aggregated and analyzed to detect threats based on defined business rules (i.e. "IF-THEN-ELSE" statements such as "IF alarms are triggered at two or more locations in category A over a given period of time, THEN send a notification to Security Operator A advising what possible incident(s) these multiple alarms may indicate and what Security Operator A should do based on the best available information, ELSE do not aggregate and send this information to Security Operator A).

118. With the Required System functionality of such IF-THEN-ELSE statements / business rules, system-generated artificial intelligence and analysis is possible and Security

well as in Volume 3."); Volume II Page 47 ("2.2.10 Data Analysis Tools The ICRS, I/CAD, and Reporting Data Analysis tools will provide means of visual presentation and statistical analysis for analysis of trends and identification of potential issues. The Lockheed Martin/ARINC Team data analysis tools enable the customer to generate and distribute standard graphic and statistical analyses of C2 operations, including center, security officer, and operator performance; workload analyses; and pin map analyses. A series of base reports as listed in the RFP will be generated. Training will be provided to enable MTA to add to the delivered reports as requirements change."); and Volume II, page 77 ("The Intergraph component of the Lockheed Martin/ARINC solution includes COTS Database support tools that provide forms generation, report generation, query creation, system administration, visual presentation, and data analysis.").

Operators would have the critical Security Information available and presented to them in a manner that would help them identify patterns and make conclusions from a reasonable starting point, rather than having to manually correlate critical Security Information from disparate subsystems, which can be difficult or impossible to do.

119. Without this critical functionality, Security Operators are less able to detect and quickly respond to a Security Incident than they would otherwise be able had Lockheed delivered and installed the Required System.

A.4. Security Operators and First Responders Lack Tools to Manage and Communicate the Limited Security Information Received

120. As reliable Security Information is received it must be properly understood, managed and communicated within a chain of command and in accordance with security operational plans.

121. The most basic security systems must be able to prioritize alarms, enable communication of Security Information between Security Operators, and otherwise support security operational plans.

122. The Required System specified these basic requirements and additional critical requirements needed due to MTA's multiple agencies, diverse assets and a multiple-Security Operator environment. These critical requirements included automated decision support tools to help Security Operators carry out response plans, and certain methods for the communication of Security Information within, between and outside of MTA Agencies.

123. For these and other functions to work properly, the Required System specified "business rules." Such business rules essentially tell the system what to do based on the receipt of certain Security Information, and are conceived to help organize, process and deliver Security Information to Security Operators in ways that follow required Security protocols and

procedures.

124. In agreeing to meet 100% of the Contractual Requirements, and in specific statements made in their RFP response, Lockheed Martin agreed to deliver a security system that would help Security Operators manage and communicate Security Information.[45] Furthermore, Lockheed agreed that they would develop and deliver the critical business rules necessary.[46]

125. The unsatisfied contractual requirements and examples cited and described below illustrate how the Lockheed System's shortcomings in managing and communicating Security Information, and its failure to deliver the required business rules, make it far more difficult for the MTA to effectively protect MTA Assets, employees and customers against Security Incidents.

[45] MTA RFP ("The Contractor shall provide networking that handles a divergent array of traffic types," "The Contractor shall provide Monitor and Control Sensors that display (e.g., graphically, textually or in tables) the network configuration, network status and identify any communication situation/problems."), *Project e-52038 RFP. Section 1AB4-eommand and eontrol (e2) Svstem*, Page 24, 25. LM RFP Response ("The C2 Systems comprise information displays, situation displays, communications interfaces, and response management tools providing multiple benefits in our integrated solutions, some of which are summarized in Table 2.2-6. These highly configurable systems receive information from various sources such as access-control, intrusion-detection, and other information systems. The C2 Systems also provide command level interfaces of these same systems as well as integration with communications systems to provide C2 operators with a seamlessly integrated work environment where they can intuitively navigate across multiple systems and information sources to implement response actions."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Pages 40, 41.

[46] MTA RFP ("The Contractor shall provide a system, which funnels Alerts/Alarms upwards according to the business rules and the Decision Support Subsystem. The Contractor shall establish the business rules by working with the agencies."), *Project e-52038 RFP. Section 1AB2-eommand and eontrol (e2) Svstem*, Page 3.MTA RFP ("The Contractor shall, as part of the design phase, work with the MTA and each Agency to develop an approach to maintaining information about resources to be used for security and/or incident/emergency response, defining the set of business rules concerning these resources and access rights to this resource information."), *Project e-52038 RFP. Section 1AB4-eommand and eontrol (e2) Svstem*, Page 20. LM RFP Response ("We will ensure smooth completion of business rules capture and concept of operations (ConOps) development through early delivery of the training equipment suite and baseline HI-ViewTM software for use during those tasks to demonstrate functionality and operational scenarios."), *Volume 1. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 2. LM RFP Response ("We utilize a structured approach for eliciting and documenting the details and business rules specific to each region and their corresponding subsidiary Agency to develop the necessary site-specific designs regarding products and localized configurations."_, *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 79.

i. Failure to Prioritize Alarms

126. The Lockheed System lacks tools to prioritize Security Information.[47] For example, if a Security Operator receives three alarms within a minute from various Subsystems (i.e. cameras, access control, motion detection), the higher priority alarms should be differentiated by an audible alert (such as a beep). Correspondingly, if any Security Information is communicated via the voice control system, the operator should be able to prioritize incoming telephone calls based on a series of defined criteria.

127. Under the Lockheed System, a Security Operator would not hear any audible alerts to help prioritize alarms and has no system tools to prioritize alarms, and the Lockheed System cannot differentiate priorities of phone calls. Using the Lockheed System, the Security Operator would be forced to attempt to manually manage the priority of the alarms and calls.

128. This inability to prioritize alarms will lead to a much slower and/or otherwise less effective response to Security Incidents than would have been the case had Lockheed delivered the Required System.

ii. Lack of Decision Support Tools

129. The Lockheed System lacks decision support tools.[48] For example, with the Required System, if a truck exploded on the Verrazano-Narrows Bridge and the incident was detected by one or more Subsystems, screens are supposed to automatically "pop up" to help a

[47] See RQMT 2534 ("The Contractor shall provide Alarm Management that provides authorized C2 Users to define the “priority” of each Alarm, Alert and Notification message."), RQMT 3408 ("The Contractor shall provide a VCS with the ability for an authorized C2 User to prioritize incoming telephone calls."), RQMT 2564 ("The Contractor shall provide different Audible Alarm, Alert or Notification indications to allow the authorized C2 User to quickly determine the criticality and location of the Alarm, Alert and Notification."); see also RQMTS 1996, 2604, 2585, 2584, 14836, 3041.

[48] See RQMT 1850 ("The Contractor shall provide a system, which funnels Alerts/Alarms upwards according to the business rules and the Decision Support Subsystem."), RQMT1902 ("The Contractor shall provide a system that, when in Emergency Mode, provides all the capability of Normal Mode allowing assessment of security incidents or potential security incidents that might adversely affect MTA operations, employees, or passengers and provide Incident Management/Decision Support capability."); see also RQMTS 1921, 1929.

Security Operator analyze the situation and make appropriate decisions to address the incident (such as what to communicate to other security operators, law enforcement personnel, and emergency responders inside and outside the MTA).

130. Because the Lockheed System lacks these required decision support tools, a security operator has no access to the security expertise that was meant to be built into the system and organized into carefully-contemplated actions to follow in order to address a wide variety of potential security incidents and scenarios.

131. Without these decision support tools, security responses are much slower and less effective than would be the case under the Required System. These problems are magnified by the Lockheed System's complete lack of a functioning Emergency Mode or Training Mode.

iii. Non-Functioning Automatic Notifications

132. The Lockheed System fails to provide functioning automatic notifications as required under the contract.[49]

133. To use an example cited above (see SectionVII.A.1.iv, supra), if a

terrorist enters a prohibited track area leading into Penn Station, the intrusion detection system of the Required System is supposed to automatically notify multiple specific people within LIRR, the MTA Police Department, and other individuals within the MTA (from a list that the Required System would allow the MTA to update) and provide each of the recipients with key data related to the alarm, such as the time or location at which it occurred.

134. The Lockheed System's inability to automatically communicate notifications

[49] See RQMT 2128.1 ("The Contractor shall provide a Command and Control System that facilitates intrusion detection notification that identifies the appropriate Agency's and its personnel to be contacted and provides alarm information concerning the potential intruder, the time of the intrusion and the location of that intrusion."), and RQMT2205 ("The Contractor shall provide a Command and Control System that is capable of displaying alarm information obtained from field devices such as electronic detectors/sensors, cameras, access controls and intrusion devices."); see also RQMTS 3199, 3200, 3201, 3202, 3203, 3636, 14541, 14523.

means that the MTA's response to a Security Incident will be slower, less effective, or otherwise inconsistent with the MTA's requirements.

iv. Non-Functioning Communications Mediums

135. The Lockheed System does not include the voice, e-mail, and video communication functionalities required by the Contract.[50]

136. For example, if a terrorist is holding an LIRR train hostage at the Jamaica Station complex, the Required System specifies the transmission of live video of the train to the NYPD so its responders can assemble an optimal response operation.

137. In its response to the RFP, Lockheed Martin specifically stated that it would provide the ability to share live video across the police community.[51]

138. Without the required ability to communicate via voice, e-mail, and video, Security Operators do not have access to all of the knowledge and information critical to the effectiveness of their response.

v. Lack of Critical Contact Lists

139. The Lockheed System does not allow for the integration and management of

[50] See RQMT 3334.2 ("The Contractor shall provide a VCS that interfaces to new and existing communications devices including, but are not limited to, various radio channels, telephone Exchange (PBX) systems, automatic ring-down (hotline) telephones, emergency phone, emergency call box devices, and paging systems currently in use at NYCT, LIRR, MNR, MTA, B&T, and LIBUS."), RQMT 1987 ("The Contractor shall provide Execution Management that supports voice communications over wired and wireless connections."), RQMT 2145 ("The Contractor shall provide a Common Operational Picture with a capability to use voice, video, data, imagery and graphics to present pertinent information on the COP".), RQMT 3704 ("The Contractor shall provide the voice, FAX, email, CCTV, and data interfaces to local agencies."); see also RQMTS 2468, 2470, 3644, 3710, 3723, 3738, 3743, 3747, 3760, 3761, 3766, 3771, 3780, 3665, 3666, 3667, 3683, 3684, 3685.2, 3886.2, 3694, 3696, 3697, 3699, 3700.2, 3701.1, 3701.2, 14814, 2158.

[51] LM RFP Response ("Our video services solution allows live video inputs from related agencies, Smart Sites, television feeds, and conferencing systems to be shared on an as needed, secure basis, in addition to allowing the selection and transmission of recorded video."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 46.

certain employee lists, contact lists, and telephone directories as required.[52]

140. To use the automatic notification example described above (see SectionVII.A.4.iii, supra), where the required protocol is to directly contact certain employees of LIRR, MTA and certain members of the MTAPD and NYPD, the Lockheed System does not provide required telephone numbers. (Moreover, the Lockheed System will not allow Security Operators to make any changes or updates to such contact lists.)

141. This lack of functionality means that critical response time will be lost while Security Operators manually find the names and contact information for critical responders and other required personnel for certain incidents.

vi. Non-Support of Response Plan

142. The Lockheed System lacks tools to support the Response Plans that Lockheed was supposed to develop to enable the MTA to most effectively and efficiently assess and direct resources in response to various Security Incidents.[53] As a result, Security Operators will be less able to effectively receive or update critical Security Information, follow the appropriate steps dictated by the applicable Response Plan(s), or assess how such Response Plans are working and

[52] See RQMT 2492 ("The Contractor shall provide the ability for the authorized C2 User to quickly determine the person to contact in each Agency, based upon the type of Incident/Emergency Situation, the day of the week and the time of day and provide their contact information."), RQMT 2502 ("The Contractor shall provide a system that provides the ability for each authorized C2 User to contact a pre-specified list of emergency response personnel at each Agency, based upon the type of Incident/Emergency Situation, the day of the week and the time of day".), RQMT 2965 ("The Contractor shall provide a Reporting capability that provides, to authorized C2 Users, a commercially available name and contact information (e.g., work phone numbers, pagers, mobile phone numbers) capability that is delivered containing the most recent complete list of MTA and agency employees, their e-mail addresses and their work mailing addresses."), RQMT 14920 ("The announcements shall include telephone numbers and names of Authority and other service personnel."); see also RQMTS: 1993, 2054, 2057, 2944.2.

[53] See RQMT 1929 ("The Contractor shall provide Incident Management/Decision Support that allows C2 Users to initiate the generation and execution of a Response Plan in response to a security event."), RQMT 1978 ("The Contractor shall provide a system that maintains a historical log of all changes to the Response Plan."), and RQMT 1929 ("The Contractor shall provide Incident Management/Decision Support that allows C2 Users to initiate the generation and execution of a Response Plan in response to a security event."). See RQMT 2001 ("The Contractor shall provide Execution Management capability that continually evaluates how well the current Response Plan is addressing the incidents/emergency situations.")

make appropriate adjustments.

143. For example, if a potentially dangerous substance is released in the Columbus Circle subway station, a Security Operator in the Local C3 Center should be able to use the IESS/C3 SoS to automatically initiate and manage an appropriate Response Plan to address the incident in coordination with internal and external MTA resources (such as the NYPD). During the response, under the Required System, the Security Operator would possess tools to update the status of the incident management and to assess progress (such as the identification of the dispersed substance, the status of passenger and MTA employee evacuation, or the arrival of first responders).

144. The Lockheed System does not include any of this required functionality, which means that Security Operators will be less effective in their response. These problems are compounded by the Lockheed System's complete lack of a functioning Emergency Mode or Training Mode.

vii. Failure to Integrate Key Business Rules

145. The Lockheed System does not integrate key business rules.[54] As described above, business rules essentially tell the system and Security Operator what to do when receiving certain Security Information.

146. For example, a breach of access control zones that occurred at two or more different subway or commuter rail stations within minutes of each other could indicate a coordinated terrorist attack. In this situation, the Required System requires that an alarm be

[54] See RQMT 2117 ("*The eontractor shall provide a eommand and eontrol Svstem that performs analvsis of alarm information to detect threats. based upon the defined business rules."). *and RQMT 2047.1 ("*The eontractor shall provide device controllers that create. aggregate and forward alarm indicators based upon pre-defined business rules and access control."*), and RQMT 1910.1 ("*The eontractor shall ensure that a message is generated and published on the message bus when a securitv event (e.g.. Incident or Emergencv Situation) occurs. based upon the business rules."*); see also RQMTS 2296.1,2419, 2420, 2424, 2426, 14919.

automatically generated and that a message be relayed to a defined user group of Security Operators based on a "business rule."

147. The Lockheed System fails to include this functionality and other business rules. As a result, situations that would be detected with the Required System will either go completely undetected or, if situations are manually detected, the response will be slower and/or less effective because critical Security Information must be manually communicated to key individuals both within and external to the MTA.

A.5. The Non-Compliant Lockheed System Does Not Allow Security Operators To Update Critical Information

148. Effective security protection requires the use of the most currently available accurate information. To keep information accurate on a security system requires that the system have the functionality whereby Security Operators can update critical items such as contact lists and response plans. To effectively use accurate information requires the flexibility for the Security Operator to interact with Security Information in a manner that supports the operational response plan.

149. The Required System specifies certain features to give Security Operators the functionality needed to ensure that contact lists and response plans could be updated. The Required System also specifies certain features to enable Security Operators to flexibly utilize Security Information in real time to update and make adjustments to Response Plans. Underlying these operational concepts are specifications that require capability and flexibility at both the system and user level (i.e. common database platform, configurable operator screens).

150. In agreeing to meet 100% of the Contractual Requirements, and in specific statements made in their RFP response, Lockheed Martin agreed to deliver a security system that

would be flexible enough to support Security Operators and protect MTA Assets.[55]

151. The unsatisfied contractual requirements and examples cited and described in this section illustrate how the Lockheed System's inflexibility makes it difficult or impossible for the MTA to effectively protect MTA Assets as required.

i. Inability to Update Critical Information

152. The Lockheed System does not allow users to update critical Response Plans, business rules, or basic information such as contact lists and telephone directories.[56]

153. For example, if during a previous fire incident, the Response Plan dictated that the MTA only contact the Fire Department City of New York, yet during the post-event review, it was determined that the better future course would be to simultaneously contact fire, police, and MTA emergency responders, the Lockheed System would not allow the relevant Response Plan or contact information to be updated.

154. Without this functionality, Response Plans will become outdated, inaccurate, and otherwise less effective in addressing Security Incidents. Again, these problems are magnified by the Lockheed System's complete lack of a functioning Emergency Mode, Training Mode, or ability to play back critical system information from the perspective of the Security Operator (see Section VII.A.1.vi, supra).

[55] MTA RFP ("The system needs to be designed such that it is flexible enough to function with missing information or conflicting information."), *Project e-52038 RFP. Section 1AB4-eommand and eontrol (e2) Svstem*, Page 16. Lockheed stated that their proposed solution "provides a flexible approach to both expansion and maintenance" and "a flexible IESS/C3 architecture that can evolve to address MTA's Concept of Operations as it is developed." LM RFP Response, *Volume 1. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 4.Furthermore Lockheed stated, "Our IESS/C3 interface engineering approach combines de facto industry standards, mature interface management, and engineering processes to make sure that external and internal interfaces are well-defined, designed, implemented, and tested, yet open and flexible to adapt to legacy, new, and evolving challenges", *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 72.

[56] See RQMT 2075 ("The Contractor shall provide Resource Management that provides a capability to interface with Agency systems that provide updated asset and resource data, as determined and documented during design stage."), RQMT 2079 ("The Contractor shall provide, where possible, automatically updated information that is obtained by Resource Management."); see also RQMTS 1945, 1946, 1970, 2068, 2091, 2923.2, 3004, 3005, 3020.2, 3021, 3023, 3024, 3025.2, 3025.3, 3027.2, 3182, 3197, 3394, 3395.2, 3397, 3406.

ii. Inability to Utilize Current Critical Information During Incident Response

155. The Lockheed System does not allow users to accept changes or data input during a Security Incident to allow current Security Information and other critical information to guide the response to the incident.[57]

156. For example, if C3 Center operators receive alarms or alerts for a trespass incident and additional Security Information indicates that the trespasser appears to be placing an explosive device, the Security Operators cannot make changes to elevate the documented incident to a higher (or, if necessary, a lower) threat.

157. This limitation of the Lockheed System could cause an incorrect or ineffective response, thus increasing the risk of injury, casualty and property damage.

A.6. The Lockheed System is Cumbersome to Operate

158. A security system should be as user-friendly as possible. To the degree that it is cumbersome to operate, a system will slow down security operations and potentially make them less effective.

159. While common sense and best practice is to deliver a user-friendly experience for every underlying functional and technical requirement, the Required System also explicitly contained certain requirements for a user-friendly experience, referenced below, which the Lockheed System lacks.[58]

160. In agreeing to meet 100% of the Contractual Requirements, and in specific

[57] See RQMT 2003 ("The Contractor shall provide Execution Management with the capability to change the Operational Mode, as warranted by the increase or decrease in severity and scope of the event."), RQMT 2004 ("The Contractor shall provide Execution Management that identifies to an authorized C2 User, any lack of information being received, gaps in the information or conflicting information and can highlight missing or conflicting information."); see alsoRQMTS 2170, 2536, 2540.2, 3022.

[58] Please note that this is by no means meant to be an exhaustive list of "user-friendly" requirements but merely two examples of unmet Contractual Requirements that lead to a cumbersome operator experience when left unsatisfied.

statements made in their RFP response, Lockheed Martin agreed to deliver a security system that would be "user-friendly" to operate.[59]

161. The unsatisfied contractual requirements and examples cited and described in this section illustrate how the Lockheed System's cumbersome nature will undermine use of the system and lead to less-effective use.

i. Lack of Function Keys

162. The Lockheed System has no function keys to allow quick access to critical functions (i.e. press F1 to send your screen to your supervisor, press F2 to open the access control system and once there press F4 to bring up a contact list).[60]

163. For example, if a threat is detected, the C3 Center operators need to be able to hit a function key to quickly obtain critical information, such as the access control system, that would provide the operators with contact lists, facility maps and transit diagrams.

164. Without these contractually-required function keys, responses to security incidents will be slower or inappropriate.

ii. Lack of "Plain English" Information

165. The Lockheed System does not provide certain critical "plain-English" information without reference documentation.[61] In other words, certain data requires a security

[59] MTA RFP ("The Contractor shall provide and configure a software FA� utility, on all console workstations located in each C3 Center that shall provide a user-friendly GUI to send and receive FA� messages from other agencies."), *Project e-52038 RFP. Section 1AB7-Interfaces.* Page 4. LM RFP Response ("Data collected during an incident are only useful in mitigating a disaster if they are available in real time and viewable through a user-friendly format while being accessible to the various levels of command. The data are of even greater value when integrated into a common operational picture that creates a complete tactical and strategic picture, thereby enhancing situational awareness for decision makers."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 36.

[60] See RQMT 2291.3 ("The Contractor shall program function keys for quick access to critical, key functions.").

[61] See RQMT 2302.1 ("The Command and Control System shall provide error messages that do not require the use of a reference document for interpretation".).

operator to turn to another source to understand the data.

166. For example, if an operator sees a message relating to "error code #," the operator's response would be delayed while s/he uses a reference document to determine the issue. If the error message was programmed to give a clear indication of the issue(s), as called for in the Required System, the security operator would immediately know how to respond to an error, which would not be communicated with a code. Without this plain English information, response to security incidents will be slower or otherwise less effective.

B. Other Major Problems with the Lockheed System

B.1. The Lockheed System Does Not Manage Critical Information as Required

i. Inability to Update Reports

167. The Lockheed System does not allow users or system administrators to provide manual updates to required reports and functions when necessary.[62]

168. For example, if a system administrator needed a report containing specific data for an audit and no pre-set reports included the required data, the system administrator would need to manually create a report with the necessary data. The Lockheed System does not include this function, as required by the Contract.

ii. Failure to Catalog and Archive Database Changes

169. The Lockheed System does not log and archive changes (including detailed event history) that are made to database information.[63] In addition, access to the detailed event history

[62] See RQMT 2180 ("The Contractor shall provide Asset and Resource Displays that provide the authorized C2 Users with the capability to update any automatically entered assets and resource data."), and RQMT 2647 ("The Contractor shall provide Equipment Trouble Reporting capability that enables data to be entered, retrieved, updated, processed and incorporated into trouble reports. No information available."), and RQMT 3232.2 ("The Contractor shall ensure the System Administrator has the ability to change (add, delete or modify) the set of functions assigned to C3 Centers, user classifications and workstations."); see also RQMTS 2455, 1918, 1919, 1920, 2363, 2620, 2621, 2623, 2648, 2708, 2711, 2712, 2714, 2715, 2716, 2717, 2718, 2719, 2723, 2737, 2751, 2761, 2764, 2766, 2768, 2771, 2773, 2774, 2775, 2758, 2770.2, 3214, 3222, 3223, 3225.1, 3230.1, 3231.1, 3236, 3241, 3242, 3250.

is not restricted to authorized system administrators, which means that Security Operators and other personnel could change, modify, or delete such event histories.[64]

170. For example, the MTA must regularly review the actions of the C3 Center operators to monitor their performance and actions during daily tasks and incidents. If the MTA cannot access archived logs of an operator's performance and actions, training or performance issues are more likely to go undetected. In addition, a Security Operator could make changes to an unrestricted database intentionally or unintentionally that could destroy or delete data critical to an investigation or review of an incident.

iii. Lack of a Common Database Platform

171. Much of the capability of the Required System to analyze, manage and communicate Security Information is based on the system functionality that is enabled by the proper implementation of a common database on which security information that comes from different sources can be correlated for the various functions of analysis, use and communication (i.e. a common database platform). The Lockheed System lacks a common database platform.[65]

172. For example, if a tunnel was chemically attacked, a notification to that effect would be received by the C3 Center. If the attacker also breached other areas protected by an access control system, a separate alarm would be received by the C3 Center. The Required

[63] See RQMT 2627.1 ("The Contractor shall ensure all changes to database information are logged and archived."); see also RQMTS 2628, 2687, 2707, 2776, 2777, 3292, 3517.

[64] See RQMT 3062 ("The Contractor shall provide security to ensure that the Data Access Log cannot be modified or deleted by the C2 Users and only the System Administrator can delete a Data Access Log."); see also RQMTS 3066.1, 3067.2, 3068, 3076, 3077.1, 3095.1, 3096.1, 3097.1, 3098, 3155, 14518, 14517.

[65] See RQMT 2608 ("The Contractor shall provide Alarm Management that logs all newly generated C2 Alarms, Alerts and Notifications to a database."), RQMT 2645 ("The Contractor shall provide Emergency Situation Notification that has two parts: first, is the creation and maintenance of a list of personnel to notify in case of an Emergency Situation and applicable procedures to follow; and second, is the creation and maintenance of information regarding emergency situation that is stored in a database that can be selectively queried for information retrieval, maintained by authorized users and allow for on screen display and printing of information."); see also RQMTS 2293.1, 3286, 3287, 3297, 3331.1, 14509.

System provides that the two alarms are to be tied together on a common database platform so that a security operator would know they are related and have the ability to obtain and provide the most pertinent information to direct a response.

173. The Lockheed System lacks this common database platform to automate the notification that multiple alerts are connected. Consequently, the MTA's response will be based on incomplete or inaccurate information and will be slower and less effective.

B.2. The Lockheed System Lacks the Required IT Security

174. The most basic security systems must effectively protect the sensitive information that they contain. Which individuals on the chain-of-command have access to certain information and functions, and the management of such access rights on a security system, are of high importance to maintaining effective security operations.

175. The Required System specified certain security protection of system information and assets, certain user-access rights and certain diagnostic tools to monitor network security.

176. In agreeing to meet 100% of the Contractual Requirements, and in specific statements made in their RFP response, Lockheed Martin agreed to deliver a security system that would be secure enough to support Security Operators and protect MTA Assets.[66]

177. The unsatisfied contractual requirements and examples cited and described in this section illustrate how the Lockheed System's shortcomings in protecting Security Information and other critical information could undermine the use of the system and lead to security

[66] MTA RFP ("The IESS/C3 shall be a secure, integrated, automated SoS designed to facilitate normal and emergency security operations across the MTA."), *Project e-52038 RFP. Section 1A-Brief Description of Work*, Page 1. LM RFP Response ("The C3 Communications and Networking Systems will be a secure, mission critical system based on industry standard protocols and equipment at the locations specified. The C3 Communications and Networking Systems will interface with the existing agencies' communication systems without degradation of current services. The C3 communications systems equipment will be overlaid with a security transport layer to insure the data integrity requirements are satisfied. The C3 communications system will transport voice, data, and video services to the command centers, smart sites and field devices."), *Volume 2. Proposal Summarv. Solicitation No. e-52038*, July 22, 2005, Page 51.

breaches.

i. Lack of Certain Login, Credentialing and Verification Functions

178. The Lockheed System does not include login, credentialing, and verification functions required by the Contract.[67] Individual C3 operators and system administrators must be accountable for actions taken while using a workstation linked to the system. Without proper login, credentialing, and verification functions, there is no accountability and no ability to limit a user's access to data and system tools specifically needed for their job responsibilities.

179. In addition, the lack of these functions makes it considerably more difficult to discern if an unauthorized user has accessed the system. This inability to restrict system access to appropriate personnel places the integrity of the IESS/C3 SoS at risk and greatly limits the MTA's ability to maintain a secure system infrastructure.

ii. Lack of Network Monitoring Tools & Capabilities

180. The Lockheed System lacks the network monitoring tools and capabilities required by the Contract.[68]

[67] See RQMT 3156 ("The Contractor shall provide Access Management that provides an audit trail for tracking system management activities such as modifying system parameters and creating, editing, or deleting user accounts with regard to login information."), RQMT 3496 ("The Contractor shall provide a system that allows logging and cataloging of individual archived video footage with relevant identifications such as but not limited to date, time, period , location of camera, facility, incident information, archival period, archive expiration date , medium identification, storage location etc."), and RQMT2509 ("Read and write access to the external server shall be permitted by authorized users only. Authorized users shall be provided a valid username and password to gain access to the external server."), RQMT 2863 ("The Contractor shall provide an Emergency Tracking Site that is only accessible by authorized C2 Users with valid security credentials (e.g., username and password)."); see also RQMTS 2092, 2102, 2872, 2871, 3121, 3138.2, 3145.3, 3146, 3150, 3151, 3162, 3186, 3187, 3188, 3579, 3580, 15410, 15404.

[68] See RQMT 2104 ("The Contractor shall provide Monitor and Control Sensors that evaluates network information and provides the authorized C2 User the ability to reconfigure the network when a communication situation/problem occurs."), RQMT 2105 ("The Contractor shall provide Monitor and Control Sensors that display (e.g., graphically, textually or in tables) the network configuration, network status and identify any communication situation/problems."), RQMT 3582 ("The Contractor shall ensure the health of all server systems are continually reported on the Network Management System (HP Open View or approved equal)."), RQMT 2517 ("The Contractor shall provide Alarm Management that provides a centralized interface - a uniform clearinghouse - for all Security-related Alarms, Alerts and Notifications."), RQMT 2787 ("The Contractor shall provide an Information Playback

181. For example, if there is a network issue to be investigated, a Security Operator depends upon the various monitoring systems to review and direct a response. Under the Lockheed System, should the underlying communications network experience problems or a service disruption, there would be no way for the security operators to ascertain the source of the failure (such as devices in the field, network connectivity, or software). In other words, with the Lockheed System, if the system goes down, the Security Operator will not be able to identify the problem.

182. Having proper sensors and alarm capabilities at the network communications layer, called for by the Required System, would allow Security Operators to act accordingly to manage connectivity while maintaining the integrity in performing their monitoring and dispatch duties.

iii. Insufficient Encryption

183. The Lockheed System lacks the encryption method that was to be provided by the Required System.[69]

184. For example, web server access to various services contained within the IESS infrastructure must be done in a secure fashion, even though the applications are contained within MTA's intranet, utilizing common Secure Socket Layer (SSL) protocol or other approved transport encryption. Such procedures ensure that the information sessions regarding the device, server, and operator stations are not tampered with and subsequent transactions will be performed securely.

185. The Lockheed System lacks this required functionality. As a consequence, the

capability that prevents alteration of real-time or existing historical data by the Playback execution or by any user."); see also RQMTS 1870.3, 2473, 2474, 2477, 2514, 3103, 3576, 3587, 3606.1, 14519, 15478, 15479.

[69] See RQMT 3254 ("The Contractor shall provide a C2 System that uses Secure Sockets Layer (SSL) or other encryption method for all web-based communications."); see also RQMTS 3273, 3275, 3276, 3279, 3294.

system is more likely to be penetrated by individuals (such as hackers) who could disrupt system operations, destroy the system software or data, or obtain critical Security Information.

VIII. Conclusion

186. The delivery of the Required System was critical to the protection of the MTA's assets. In my opinion, had the Required System been delivered by Lockheed, the MTA would have been far better able to protect its assets than it is now able to do with the Lockheed System. In my opinion, the consequences of the shortcomings between the Lockheed System and the Required System are potentially severe.

187. The Required System was intended to support and enhance the capabilities of individual Security Operators and First Responders, as well as teams of individual Security

188. Operators were supposed to be organized in a chain-of-command. Under the Required System, the Security Operators were to be provided with complete, accurate and reliable Security Information and they were to have the capability to rapidly and effectively manage, communicate and act upon such information according to appropriate plans, protocols and procedures. These goals were to be achieved by meeting the Contract's technical requirements, which specified critical features, functionality, modes, security and other aspects of the Required System that Lockheed agreed, without exception, to design, test, implement, support and maintain, and to train the MTA how to use.

189. In my opinion, the requirements that Lockheed failed to meet, as reflected in the Project test records and my own observations of the system, are extremely significant. As set forth in Section VII.A, the Lockheed System does not provide Security Operators and First Responders with complete and reliable information as required; and it does not provide Security Operators with the ability to receive, communicate and input information in a timely, accurate

and effective manner. The Lockheed system is also missing crucial modes for training and, as set forth in section VII.B, maintenance and support, as required. The result of these deficiencies is that in the event that serious Security Incidents occur, more people will die or be injured, more property will be damaged and MTA operations will be interrupted for longer periods of time from certain terrorist and other incidents than if Lockheed had complied with the Contract.

190. Whether considered for its capability, functionality, training, maintenance or support, the system required by the Contract was supposed meet the MTA's immediate and future need to adequately protect its assets. Absent significant additional effort and expense on the part of the MTA, the Lockheed System does not meet the needs of the MTA yesterday, today or tomorrow.

REBUTTAL TO THE AELLA/DESTEFANO REPORT

I. Executive Summary

191. I have reviewed the Initial Expert Report Concerning Physical Security Technology Integration and Testing by Aella Consulting Group, Inc. ("ACG") and Louis T. DeStefano, Inc. ("LTD"), dated June 21, 2011, prepared for Lockheed Martin (the "Aella/DeStefano Report").

192. This response to the Aella/DeStefano Report is based on my analysis of facts, documents, and principles that are generally understood and accepted by those who create and install security technology projects that support security operations. Where it is not otherwise indicated, this declaration is based on my experience both as a customer of functioning security systems and as a consultant in the security consulting business.[70]

193. First, it is my opinion that, contrary to the conclusions of Aella/DeStefano, a vendor in the security industry is expected to fulfill contractually required technical specifications. Contrary to the arguments of the Aella/DeStefano Report, this fundamental principle is not excused (or altered) by the method by which a project is procured and managed, the complexity or simplicity of a project, or the vendor's decision to wholly or partially integrate commercial off-the-shelf ("COTS") products or custom hardware and/or software into a compliant solution.

194. Second, this declaration rebuts the arbitrary, non-contractual, testing status categories created by the Aella/DeStefano Report that purport to represent documented testing failures as something other than failures.

[70] My experience as (i) a government customer of security systems (NYPD, US Marshals Service, FDNY), (ii) consultant for the design and implementation of Security Systems (SafirRosetti and VRI), and (iii) as a board member of companies involved in security technology (Verint Systems, Lexis--- Nexis Special Solutions, Implant Sciences) is further specified in Exhibit A of my Initial Expert Report.

195. Third, this declaration discusses the importance of the requirements that ACG and LTD acknowledge did not pass testing. While the Aella/DeStefano Report generally dismisses these failures as inconsequential, in my opinion, many of these failed requirements are critical to the viability of the project.

196. Finally, this declaration highlights aspects of Lockheed Martin's RFP response, project management plan, and actual project management practices that rebut the Aella/DeStefano Report's erroneous factual assumptions and conclusions that Lockheed effectively designed a contractually-compliant solution.

197. In sum, this declaration rebuts the Aella/DeStefano Report's overall opinion and demonstrates that Lockheed did not properly deliver the contractually required system (the "Required System"). Because I detailed the myriad shortcomings of the Lockheed System as evidenced in the documented testing record and confirmed by my observations above, I will not fully restate those details here. Rather, I will draw on select examples that directly address issues raised in the Aella/DeStefano Report, which will further highlight the multiple ways that Lockheed failed to deliver the Required System and the severe consequences that resulted.

II. Facts and Data Considered for this Report

198. I considered the following sources of information in rendering my opinion:

1. My direct observations of the Lockheed System made at various times at the MTAPD Central C3 Center at Long Island City and the Long Island Rail Road regional C3 center at the Jamaica Station Complex;
2. The Project RFP and Contract (including Lockheed Martin's proposal response to the RFP);
3. The Project test records;

4. Interviews of MTA security professionals, MTA engineers, MTAPD officials and MTACC Project representatives (including engineers and project managers from Parsons Transportation Group/Parsons Brinkerhoff joint venture and Dnutch, Inc.)[71];
5. The Concept of Operations and Business Rules as drafted;
6. The Aella / DeStefano Report;
7. The Dnutch Report.

III. The Importance of Project Requirements[72]

199. A vendor's fulfillment of contractually-required technical specifications is critical to the successful implementation of a security system, regardless of whether the project is conceived and managed as "design-build," "design-bid-build," or otherwise.[73]

200. This is true regardless of the use or non--use of COTS products in the project solution[74] and regardless of the level of integration among various software systems required by

[71] Such personnel include Joseph Christen, MTACC; Ronald Pezik, MTACC; Kenneth Shields, URS; Terrence Fetters, Parsons; Shirsh Gupte, Parsons; William Morange, MTAPD; Ronald Masciana, MTAPD; Ernest Pucillo, MTAPD; William Coan, MTAPD; Ray McDermott, MTAPD; Leonard Viviano, MTAPD; Howard Reith, Dnutch; Robert Murphy, LIRR; John Hyland, LIRR; Sean Ryan, MNR; April Panzer, MNR; Lisa Schreibman, NYCT; Staff at GuidePost Solutions.

[72] My opinions in this section are based on my own extensive experience as well as the depth of experience possessed by others at Guidepost Solutions, who have ensured that security systems procured for critical facilities are properly developed, implemented, and integrated to support effective security operations. Examples of such client engagements include those on behalf of Keyspan (60 facilities); LDS Church (25 facilities); Electronic Data Systems (EDS) (40 facilities); Digital Realty Trust (40 facilities); SalesForce.Com (20 facilities); Yankee Stadium (1 facility); and New Meadowlands Stadium (1 facility).

[73] Project C---52038's title "Design, Development, Furnishing, and Installation of an Integrated Electronic Security System (IESS) and Security Operations (C3) Centers at Various Locations" (emphasis added), the use of the word "develop" throughout the "Brief Description of the Work" of the project in the Request For Proposals ("RFP") (see Requirements, 6,10, 15 ,31, 32, 34, and 36), as well as any reasonable interpretation of the technical specifications discussed herein (see Section III below), make it clear that the contractor is responsible to both design and develop the Required System (as well as install and maintain it). It is generally understood in the security industry that a "design---build" project, in the context of a software---based project means design and development.

[74] This principle generally applies whether or not software development is required by either the integrator or the COTS vendor(s) who support the integrator's solution and regardless of any contractual provisions requiring the customer to approve software development that may be required to deliver a solution.

the vendor's solution to meet technical requirements.

201. Indeed, in the security industry, where the requirements of security operators are often highly specific to their physical, IT, and threat environments, COTS products are often a common starting point for a project. Such systems typically do not meet all contractual requirements "out of the box" and require highly specific configuration and/or software development to meet such requirements.

202. Compliance with requirements and effective system integration are especially important for a "system of systems" project such as Project C-52038, conceived to protect the vast MTA transit system and its people, assets, and critical operations across multiple agencies, locations and operating requirements.

203. Rather than serving as a conceptual starting point from which a vendor can arbitrarily deviate, technical specifications are generally understood in the security industry to be an anchor to the reality of a project's goals and promises –moveable only on a limited-exception basis by the willing contractual consent of the customer and the responsible vendor.

204. Contractual technical specifications for a security project thus essentially serve as the "bottom line" in communicating what the system must be able to do at a functional level and how this functionality must ultimately be delivered, implemented, and otherwise supported throughout the lifecycle of the project and thereafter.

205. On "design-build" projects, not only does the vendor assume full contractual responsibility for testing, delivering, and supporting the hardware, software, and infrastructure required to meet the technical specifications, but the vendor is also responsible for the very design that creates the technical framework and system architecture that, when properly developed and delivered, enables the project solution to meet the technical requirements.

206. Thus, the technical requirements included in an RFP such as Project C-52038 do not specify a step-by-step approach to how the vendor must satisfy them, but instead specify what the vendor's solution must ultimately be able to do to be deemed contractually compliant, and the critical milestones that must be satisfied over the project's development to prove the system's compliance with the contract.

207. Technical requirements vary depending on the project. They generally contain very basic, general requirements of what a system must be able to do.[75] They also frequently include customer-specific functionality based on the nature and scale of security threats, risks, and vulnerabilities facing a particular customer,[76] the size, capabilities and training of the staff that will operate and interact with the security system,[77] and other factors that may include how the new security system is conceived to interact with legacy and other systems to achieve security and emergency management goals.

208. In this case, the Contract includes both general and specific requirements for the Required System's functionality, performance, and operation that Lockheed was both contractually obligated to fulfill and, based on common and accepted practice in the security industry, could have and should have fulfilled.

209. Starting with the very act of responding to an RFP such as Project C-52038, a

[75] See, e.g., RQMT 6 ("The security system operation shall be developed such that it complements the Agency's current operation and does not burden them") and RQMT 7 ("The system shall be designed to protect the MTA and its Agencies' vast network of infrastructure spanning their entire service area that provides public transportation services (buses, subway, rail, and tunnels and bridges for vehicular traffic)").

[76] See Section V.C of my Initial Expert Report (discussing the Threat, Risk & Vulnerability Assessment completed by MTA in fall 2004).

[77] See, e.g., RQMT 3 ("The C3 Centers shall provide security personnel with a comprehensive Situational Awareness (SA) and help responders coordinate their actions during an incident"), RQMT 9 ("The IESS/C3 system shall address the needs of such multi---operational multi---jurisdictional scenarios for proper operation and response"), and RQMT 3323 ("In order to help coordinate activities between agencies, operators, field personnel, and others, a Voice Communications System (VCS) shall be required").

proposer who intends in good faith to meet a project's technical requirements must do the requisite work to thoroughly understand the project's technical requirements, develop a solution that will meet the requirements, and communicate to the potential customer any requirements that it will not be able to meet.

210. During the course of contract negotiations, the proposer/prospective vendor has additional opportunities to negotiate the removal or modification of technical requirements that it cannot meet or otherwise believes should be altered. Once the proposer has been selected and the negotiated, the contract is signed and the project begins, technical requirements should only be altered on an extremely limited-exception basis with the mutual consent of the parties (pursuant to a contractually-controlled waiver process). If the technical requirements are unilaterally altered by the vendor (or the customer) outside the contractually dictated process, the very sanctity of the project contract – including the reasons the vendor was selected in the first instance and the ultimate ability of the project to achieve operational goals – can be severely compromised.

211. Although the arguments and appendices of the Aella/DeStefano Report suggest that the COTS-based nature of Lockheed's solution excuses Lockheed from complying with critical technical requirements, Lockheed was very clear in its RFP response that it intended to meet 100% of Project C-52038's requirements.[78]

212. Lockheed made further representations in its RFP response that its solution (then called HiView^{TM}) (i) would provide great operational benefit for the MTA[79]; (ii) was based on

[78] See Lockheed Proposal, Volume I, page 17, "The Lockheed Martin/ARINC Team takes NO contract exceptions. Our proposed offering is 100% compliant with MTA Capital Construction Company's Request for Proposal" [no emphasis added],; and page 19, "Our proposal takes no exceptions to the contract and is 100% compliant with the requirements of the RFP."

[79] See Lockheed Proposal, Volume 2, page 1, where Lockheed states that its IESS/C3 Solution "will enable a smooth system deployment to meet MTA's operational need for world---class physical security"; page 4, "The

Lockheed's rigorous review of Project requirements[80]; (iii) was based on a rigorous study and the proper due diligence in selecting appropriate COTS products[81]; (iv) was properly developed in concert with vendors of COTS products to ensure 100% compliance with project requirements[82];

Lockheed Martin/ARINC Team's IESS/C3 solution addresses the diversity of MTA's operational modes and Agency---specific challenges through architectural flexibility, COTS configurability, and collaboration with stakeholders in codifying their business rules"; and throughout the RFP response where Lockheed represents that its solution will enable decisions to be made in real---time, and will provide advanced "situational awareness" and interoperability between agencies and with entities outside of the MTA (i.e. "operator---centric view [that] places the right information, in the right place, at the right time to assist the operator in making a decision about an event or group of events that are taking place in real time" (Volume II, Page 4); the ability for the system operator "to intelligently reach into any available Monitored Location providing the necessary situational awareness to manage events as they develop" (Volume II, Page 12); "Each C3 Center shall be configured to allow for autonomous operation, while at the same time the SoS shall facilitate information exchange between Central C3 Center, Regional C3 Centers, and local/remote C3 Centers based on predetermined business rules and access rights." Volume II, Page 37).

[80] See Lockheed Proposal, Volume I, page 1, "We understand MTA's requirements and the skills needed to complete the Project within budget and on schedule" [no emphasis added]; page 16, "The Lockheed Martin/ARINC Team has been working with the MTA for more than three years to gain a detailed understanding of the program and associated risks. To ensure on--time project completion, we have developed a strategy to mitigate known risks and identify potential risks far enough in advance to avoid serious delays and rework."[no emphasis added]; Volume II, Page 6, "Our IESS/C3 functional architecture reflects a thorough review of MTA's RFP and the decomposition and repartitioning of the functional requirements. Our analysis has enabled the Lockheed Martin/ARINC Team to take a creative approach to the integration of the C2, Smart Site, and Monitored Location subsystems and ensure that we deliver the full benefit of an integrated physical security system."

[81] See Lockheed Proposal, Volume 2, page 29 "Our integration---focused, system---engineering---driven organization, conducts a market analysis and product selection or trade study to choose the core system components that best satisfy a particular customer's requirement set as our first step in any COTS---based project. As depicted in Figure 2.1---10, we performed a trade study in the form of a market survey and evaluation for the MTA IESS procurement in order to select the core system elements that best meet or exceed the requirements and overlying objectives of the MTA RFP"; and page 32, "Our study was designed to select the best possible technical solution available and overall value to MTA. To this end, the trade study relies on information from internal sources, such as our experienced engineering and fielding staff, as well as external sources such as manufacturer representatives, engineering staff, public domain data, and VAR agreement---based documentation.

Although Lockheed Martin has developed relationships with some COTS providers in the security industry, including VAR agreements, our primary select criteria were driven by our desire to satisfy our customers' requirements and long---term supportability needs. "

[82] See Lockheed Proposal, Volume 1, Page 4, "Lockheed Martin, Intergraph, and Lenel have jointly developed this solution to meet evolving security market requirements"; page 5, "Lockheed Martin, Intergraph, and Lenel bring the expertise needed to configure the HI---ViewTM integrated suite of products to meet MTA's broad range and agency---specific security and command, communications, and control operational needs. We have defined and implemented the interfaces between the C3/CAD, access control, and video surveillance products that are the core of the system";and page 12, with a questionable representation that ultimately proved to not meet Project Requirements, "Because integration with Intergraph and Lenel software into HI---ViewTM has been accomplished, the field integration process will only require setting up specific screen layouts and populating databases with specific addresses and configurations of the access control panels, intrusion detection devices, and CCTV equipment"; also in Volume II, Page 1, "The Intergraph Public Safety I/CAD product suite, as integrated within HI-

(v) was based on successful implementation of HiView on similar projects[83]; and (vi) would be developed and delivered with the same level of rigor and process controls that Lockheed typically applies to custom software development.[84]

213. In sum, Lockheed did not present its COTS-based solution as the limited non-compliant Lockheed System that the Aella/DeStefano Report wrongfully opines to be acceptable, but as a fully-compliant solution that would be so useful and successful that the MTA security operations would greatly benefit from its use and could even share revenue in selling similar systems to other transit agencies.

214. The HiView^{TM} COTS-based solution that Lockheed proposed was not a requirement of Project C-52038, but rather one of Lockheed's selling points based on: (i) its representations of the purported actions it took to develop the HiView^{TM} solution; and (ii) the actions that Lockheed represented that it would take to implement the HiView^{TM} Solution once

--ViewTM, supports the requisite C2 functions, CAD, and interfaces to the other solution elements. Linked to Intergraph within HI---ViewTM, the Lenel Systems OnGuard® products provide for the IESS level of control and management for operation of the access control, intrusion detection, less---than---lethal devices, and local video systems. Video surveillance is supported by a mix of Pelco/NICE products, with video storage managed through a mix of NICE/EMC products. Our selected core components of the communications systems come from industry leaders Penta and Cisco."

[83] See Lockheed Proposal, Volume 1, Page 5, "Lockheed Martin, Intergraph, and Lenel bring the expertise needed to configure the HI---ViewTM integrated suite of products to meet MTA's broad range and agency---specific security and command, communications, and control operational needs. We have defined and implemented the interfaces between the C3/CAD, access control, and video surveillance products that are the core of the system. Lockheed Martin's relevant surveillance, intrusion---detection, and access---control expertise includes working with Lenel at the PA NY/NJ's Hudson River crossings and NICE at FBI Headquarters. LM has also worked with the following additional video analytics (smart camera/intelligent video) providers over the past four years: Verint (formerly Loronix) at PA NY/NJ; Safeguards at Forts Myer and McNair; Sarnoff Laboratories at Fort Belvoir (Combat Zones That See); GE Security at the GE Research Center; Object Video in pursuit of PA NY/NJ Perimeter Intrusion Detection System (PIDS); Broadware at a classified customer location; and Guardian Technologies. LM is also the primary systems integrator of CSI for the London Metropolitan Police."

[84] See Lockheed Proposal, Volume 1, Page 5, "Overall integration and deployment is based on LM's mature SEI SE/SW CMMI Level 5 processes and leverages our Team members' core competencies to ensure high---quality, comprehensive solutions to meet all requirements."; and Volume II, Page 91, "Following the same structured approach to meeting requirements that improve quality of developed software will allow the Lockheed Martin/ARINC Team to ensure the development of the Agency Business Rules, and subsequent system configurations will address MTA's defined missions."

awarded the contract.[85]

215. It was perfectly reasonable for the MTA to rely on Lockheed's representations that it would deliver a fully compliant solution utilizing the COTS products it selected.

216. Lockheed's representation that the IESS/C3 System would be built with COTS products did not limit Lockheed's need to provide 100% compliance with the contract requirements.[86] In the security system industry, it is well known that the vendor team is required to fulfill all of the contract requirements, whether through COTS products, software development or configuration.[87]

217. For example, a client of SafirRosetti that built and now operates a large stadium issued an RFP with specific technical requirements related to the functionality of video necessary to support security operations. When the COTS-based solution that the system integrator proposed (and the client accepted) failed to deliver the required functionality, the system integrator proposed an alternative COTS-based solution. Upon client acceptance of the alternative solution, the integrator successfully implemented that solution, which was based on

[85] See Footnote 82 above.

[86] In fact, the Aella/DeStefano Report creates a false dichotomy between 'COTS systems' and 'custom systems." For example, the SAIC Proposal for the IESS Project stated: "The solution proposed by the SAIC Team is primarily an all COTS product suite. Software development will be required for COTS product interfaces and the IESS Simulator and Data Validation modules. SAIC estimates approximately 55,200 Source Line of Code (SLOC) will be developed for the MTA project. Approximately seven thousand SLOCS are estimated to be required for functional applications which will serve as "plug ins" to work in combination with COTS. The remaining 48,000 SLOCs represent code development for interfacing 45 COTS Applications and 28 COTS Management Systems." Again, the goal is to furnish a 100% compliant system. Whether Lockheed would be able to do so without undertaking software development was its own challenge. But certainly, the expectation in the industry is that a COTS---based system, which is what the IESS/C3 Project was, would need to be enhanced with some software development to meet the requirements of a Project such as this. (SAIC Proposal "Overview of Software Development, Integration and Deployment Approaches", Page 6---1).

[87] In the case of the Project C---52038, the RFP clearly contemplated software development as a likely activity, regardless of whether or not the vendor decided to use a base of COTS products. See, e.g., RQMT 15 ("Various activities involved in this project include but shall not necessarily be limited to the design development, proto---type testing, furnishing and installation, software development and systems integration, training, testing and commissioning") (emphasis added); also, section "1AB11, Software" (RQMTS 4218 through 4246) specifies software development processes, procedures, documentation and other requirements for both COTS and non---COTS based software.

different COTS software and hardware than what was originally proposed and accepted. The new solution provided the relevant contractually–required functionality that was missing from the originally–proposed video system.

218. Contrary to the Aella/DeStefano Report's contention that the MTA was unreasonable in its expectation of a properly integrated system that worked to the benefit of security operators[88], Lockheed was very clear in its RFP response that its solution would enable great operational benefit with a "fully integrated" solution[89].

219. In the security industry, the term "integration" means two or more otherwise disparate systems being made to work in concert to achieve a specified purpose.[90]

220. Contrary to the statement in the Aella/DeStefano Report of a "common misunderstanding" between "interfacing" and "integration,"[91] I have never heard or used the term "interfacing" as an acceptable proxy or synonym for the word "integration." The mere fact that two or more systems somehow interact with each other (i.e., "interface") does not mean that

[88] See Aella/DeStefano Report Section II. B, starting at Page 10, where the report improperly concludes that COTS was a requirement of the Project and improperly contrasts COTS projects with custom solutions where "the user gets exactly what they want" (page 11); Section II, D. where the report opines that "MTACC should not have been surprised by limitations imposed by the selected, and later approved, COTS products" (page 13): Section III.D which improperly compares the Required System to Microsoft Windows and improperly opines that the statement "a user has to live with the standard feature set developed for everyone in the community" properly applies to the Project (page 17); Section III.B.4, which improperly implies that merely interfacing Lenel and Intergraph would be sufficient to meet applicable requirements (page 25) and meeting the RFP requirements could be accomplished by defining the business rules of each MTA agency (or "matching them as close as possible") based on "the limitation from using COTS products" (page 26).

[89] See Lockheed Proposal, Volume 1, Page 12, "LM/ARINC will deliver to MTA a fully integrated solutions package applicable across all Agencies"; Volume II, Page 17, "At the heart of our IESS is Lenel Systems' On---Guard solution. This COTS product solution is fully integrated downward to provide 100 percent control of all Smart Site and Monitored Location edge sensing devices and systems, such as Pelco, NICE, EMC, and intrusion---detection and access---control peripherals. Similarly, it is fully integrated upward to provide a seamless interface of information to our C2 Intergraph suite."

[90] For example, the SAIC Proposal for the IESS project defined "Integration Approach" as "the activities related to the bringing together of configured COTS products, computing hardware, and sensor equipment to meet the MTA requirements and performing validation of the integrated components in a unique test environment" (SAIC Proposal, Volume I, Page 11).

[91] See Aella/DeStefano Report page 25.

they are properly integrated.

221. For example, the fact that an access control system and a camera system utilize an Application Programming Interface ("API") by which they can communicate (i.e. they have an "interface") does not mean the systems are properly integrated. The Aella/DeStefano Report's false distinction between "integration" and "interfacing" does not excuse Lockheed's failure to meet specific project requirements.

222. The ability of a Security Operator to retrieve information from disparate systems at a single point of interface is merely one of several critical layers in achieving the level of integration that Lockheed was contractually required to deliver.

223. As a result of Lockheed's failure to integrate the various products, many of the automated, intelligent functions of the Required System, which were intended to support the operator and deliver the conceived benefit of the Required System as a force-multiplier, were either severely lacking or not delivered at all.

224. Based on the RFP and Lockheed's response to the RFP, accepted industry practice, and available technology, it is clear that Lockheed was responsible for and should have delivered a solution that met the IESS/C3 Project's technical requirements. The fact that Lockheed may have faced technical challenges based on the COTS products that it chose is not a reasonable or acceptable excuse for non-compliance.

IV. The Impact of Lockheed's Failure to Complete the Testing Process and Meet Technical Requirements

225. This section rebuts the arbitrary way in which the Aella/DeStefano Report presented testing failures as something other than failures and details the consequences of those specific shortcomings of the Lockheed System. It further explains the significance of the failed requirements that the Aella/DeStefano Report admits are failures but generally dismiss as

inconsequential. Before discussing these failures, I will give a brief overview of project testing, to emphasize its criticality to Project C-52038.

A. Overview of Project C-52038 Testing Process

226. Testing is important to every electronic security system project, and typically serves as the primary method to validate the system's ability to provide all of the required functionality.

227. It is critically important that system tests are conducted in a manner that validates both the literal plain meaning of each individual requirement and the technical and common sense context in which satisfying each requirement supports the overall functionality of the system. Thus, the best practice for a testing program is not only to test each requirement individually, but also to test logical groupings and overall system functionality to ensure both that individual requirements are satisfied and that the system functions effectively as a whole.

228. Testing is conducted in both controlled environments (e.g., normal room temperature, sufficient lighting, normal humidity, a small subset of potential users and user IDs) and, as applicable, in environments that simulate more challenging conditions (e.g., extreme temperatures, low lighting, high humidity, a full set of users and user IDs).

229. Decisions of how, when, and where to conduct security systems tests are also often affected by practical considerations related to IT network management.

230. For example, before a client expends the financial and human capital necessary to place a security system on a live IT network, the responsible IT director may require assurances that: a) the security system functions as required; and b) the security system will not overburden, compromise, or otherwise negatively impact the overall IT network.

231. It is important to ensure that a new security system is tested and proven effective

in a “safe” environment before it potentially wastes time and money or does harm when implemented in a “live” environment.

232. For Project C-52038, as per section 1AB12 of the Contract, and further referenced in the Test and Evaluation Master Plan (“TEMP”) prepared by Lockheed, this conceptually-safe testing environment was the Factory Acceptance Testing (“FAT”) that occurred at Mitchell Field.

233. As logic and best practice in the security system industry dictate, FAT is required to be completed before a systems integrator can move on to other phases of testing. In this case, FAT was conducted in various “waves” that tested groupings of individual requirements based on the Lockheed System’s underlying COTS-based software products (e.g., Intergraph, Lenel, Broadware, etc.).

234. Lockheed’s testing was not appropriate for a security system. Instead of validating how Intergraph (the primary software interface used by security operators) would receive and communicate Security Information, Lockheed tested various system components in a vacuum. (It is remarkable that even in such a vacuum, Lockheed was unable to pass huge numbers of the FAT tests.)

235. I believe that Lockheed’s failure to explicitly test the integration of the various subsystems in FAT did not comply with accepted industry best practices and was a missed opportunity to more accurately test individual contractual requirements in proper context of what the system was supposed to do. Unfortunately for the MTA, this failure was consistent with Lockheed’s incorrect position (as echoed in the Aella/DeStefano Report) that such subsystems did not need to be integrated to meet many of the contractual requirements.

236. In my opinion, this missed opportunity further contributed to a result where

security operators cannot receive, rely upon, understand, communicate, or secure Security Information as required by the project's specifications.[92]

237. The next phase of project testing – dictated both by the Contract, Lockheed's TEMP and industry standards to take place after the successful completion of FAT – was to be Site Performance Installation Testing ("SPIT").[93]

238. As set forth in the TEMP, SPIT was a series of tests to ensure that security equipment installed at various sites was properly connected, had proper power, and functioned as required. SPIT was not completed at the time of Termination.[94]

239. The next phase of testing under the Contract and Lockheed's TEMP was Site Integration Systems Testing ("SIST"). SIST was supposed to test the System's functionality under actual operating conditions with security devices actually deployed for various agencies in the field. Despite critical testing failures in FAT and the failure to complete SPIT, Lockheed did conduct limited SIST testing before Lockheed was terminated. As further detailed in Sections B and C below, SIST confirmed (and expanded) the list of critical system shortcomings discovered in FAT.

240. Finally, the fourth progressive phase of testing on the program, per the Contract, TEMP and industry standard, was to be Systems of Systems/Acceptance Testing ("SOS/AT"), which was to occur once SIST was successfully completed. SOS/AT was supposed to ensure that the overall system functioned as required, both within and across agencies. Due to the extensive FAT and SIST failures, Project C-52038 never reached the stage at which SOS/AT could be

[92] Sections III. B and III. C below provide my analysis of the failed FAT requirements that the Aella/DeStefano Report mis---categorizes or downplays, as well as my analysis of the requirements that the Aella/DeStefano Report agrees did not pass testing.

[93] TEMP at page23 ("Prior to entering Phase 2, FAT will be completed for the components or subsystems being deployed in Phase 2.").

[94] 25 IESS MTA---CCM/LM – 01634 (the "Default Letter" from MTA to Lockheed Martin), dated May 26, 2009.

conducted.[95]

B. Lockheed and the Aella/DeStefano Report's Creation of Testing Status Categories and The Importance of the Corresponding Requirements That Lockheed Did Not Pass

B.1. My Opinion Regarding the Creation of Testing Status Categories

241. Both during the testing process, and again in the Aella/DeStefano Report, Lockheed has created new categories to describe test results in a manner that was neither authorized by the Contract nor sanctioned by Lockheed's own TEMP.

242. During the project, Lockheed unilaterally created two categories, "Non-Statused" and "Dispute," that did not exist in the TEMP. "Non-Statused" referred to contractually required items that were not tested because it was generally acknowledged that they would fail.[96] "Dispute" referred to failed requirements that Lockheed believed should have passed testing, notwithstanding the fact that the test was recorded as having failed.[97]

243. The Aella/DeStefano Report opines that the "Non-Statused" and "Dispute" categories are appropriate, despite the fact that there is no contractual support for these categories and they were not included in Lockheed's TEMP.[98] The Aella/DeStefano Report goes further and creates additional categories for non- passed requirements:[99] "Functionality

[95] The TEMP specifies that testing is to proceed sequentially – from FAT to SPIT to SIST to SOS/AT. See TEMP at Page 28, 4.1 ("The IESS/C3 SoS and its operating environment is a complex set of site and control center operations that has a large amount of test scenarios. Consequently, a hierarchy of tests (component, subsystem, system) will be performed to ensure that functionality and performance is verified.") (emphasis added). The TEMP's provisions regarding the sequence of testing reect, as it must, the terms of the Contract, which sets forth the development phases for the Project, including the sequential testing testing phases. See Specificartion Section 1AB12.2.

[96] See Aella/DeStefano Report at 68.

[97] Id.

[98] Id.

[99] "Non---Passed Requirements" refers to technical requirements that according to the testing record, Lockheed did not pass. These include requirements that Lockheed failed, requirements that were deferred and requirements that

Demonstrated," "Unwritten Expectation," and "Limitation of Approved Design."

244. I believe that the creation of the "Dispute" category was not only unacceptable according to standard practice in the security systems industry, but was also counterproductive to the successful completion of this project.

245. The TEMP made no provision for allowing Lockheed to "dispute" test results. The project had a Commissioning Agent, Systra, to provide independent and impartial oversight of the testing. Furthermore, the Contract specified that testing requirements could only be waived by the customer.[100]As I discussed above, the customer should only be asked to waive a requirement in exceptional circumstances.

246. Lockheed's creation of the "Dispute" category undermined this principle and effectively added a confusing, unreliable and contractually meaningless "second set of books" to the official testing record.

B.2. My Opinion Regarding the Unauthorized Testing Status Categories in the Aella/DeStefano Report

247. In addition to my disagreement with the very creation of categories not authorized by the TEMP, I also disagree with the Aella/DeStefano Report's application of new categories for requirements that had not passed during testing. Specifically, the Aella/DeStefano Report assigned non-passed requirements to new categories including "Functionality Demonstrated," "Unwritten Expectation," "COTS Program Restriction/Limitation," "Conflicting Specification,"

Lockheed has attempted to re---categorize into something other than non---passed requirements (i.e. "failed dispute").

[100] See, e.g., Article 8.01 of the Terms and Conditions of the Contract, "The Engineer as representative of the Authority, shall determine in the first instance all questions of any nature whatsoever arising out of, under, or in connection with, or in any way related to or on account of, this Contract including without limitation: questions as to the value, acceptability and fitness of the Work; questions as to either party's fulfillment of its obligations under the Contract, negligence, fraud or misrepresentation before or subsequent to acceptance of the Proposal; questions as to the interpretation of the Specifications and Contract Drawings; and claims for damages, compensation and losses."

and “N/A for FAT.”

248. These classifications are erroneous and misleading. In reality, they simply indicate that Lockheed failed to deliver required functionality.

B.2.1. “Functionality Demonstrated”

249. The Aella/DeStefano Report re-categorizes 130 requirements that failed under FAT and SIST and deemed those failures as having “passed” under the category “Functionally Demonstrated,” based on LTD’s opinion that “the wording and intent of the requirement had been shown.”[101]

250. ACG and LTD could not have determined that the functionality demanded by these requirements was demonstrated based on the testing record from Project C-52038. The testing records recorded these requirements as having failed.

251. Lockheed’s failure to pass this particular subset of requirements results in a system where user-entered data cannot be validated as required,[102] Security Operators[103]

[101] See Aella/DeStefano Report at 79.

[102] Project Requirements relevant to data validation that the Aella/DeStefano Report categorizes as “Functionality Demonstrated” that did not pass FAT include those requiring the Contractor to provide:

> 1) “a Command and Control System that makes extensive checks on user entries to detect potential errors” (RQMT 2300);
>
> 2) a “Command and Control System shall provide error messages that do not require the use of a reference document for interpretation” (RQMT 2302.1);
>
> 3) “Command and Control System shall provide error messages that do not require the use of a reference document for interpretation” (RQMT 2302.3);
>
> 4) “Command and Control System shall provide error messages that do not require the use of a reference document for interpretation” (RQMT 3231.1);
>
> 5) “a C2 System that alarms a condition where a modification to the function access assignments would leave one or more functional capabilities unassigned to any C3 Center, workstation and/or user classification” (RQMT 2302.4); and

may be unaware of non-functioning security devices and/or processes,[104] and the security information that is conceptually available cannot be accessed,[105] managed,[106]

6) "a C2 System that alarms a condition where a modification to the function access assignments would leave one or more functional capabilities unassigned to any C3 Center, workstation and/or user classification" (RQMT 3231.2).

Project Requirements relevant to data validation that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass MTAPD SIST include those requiring the contractor to provide:

1)" Execution Management that identifies to an authorized C2 User, any lack of information being received, gaps in the information or conflicting information and can highlight missing or conflicting information" (RQMT 2004); and

2) "Execution Management that prompts authorized C2 Users for missing information, allowing them to enter complete or partial information in response (RQMT 2005, also failed B&T SIST).

[103] "Security Operators" as used in this declaration means both actual users and beneficiaries of the security system conceived in Project C---52038.

[104] Project Requirements relevant to making Security Operators aware that a device or process may not be functioning that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass FAT include those requiring the contractor to provide:

1) "Failure Notifications that include errors that the archival hardware or software or the associated software application had a failure (e.g., data from online storage has not been successfully transferred to archive") (RQMT 2472);

2) "an Archival capability that is monitored for failures and when they occur" (RQMT 2473.1);

3) "that each authorized C2 User can initiate equipment trouble reports" (RQMT 2468);

4) "a Failure Handling Log that is viewable by System Administrators only" (RQMT 3067.2);

5) "security to ensure that the Failure Handling Log cannot be modified or deleted" (RQMT 3068); and

6) "that the failure of any interface (line, console, network) leading to a loss of communication shall be alarmed and immediately displayed to authorized C2 Users" (RQMT 3683).

Likewise, an important device failure notification Requirement that did not pass B&T SIST that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" is RQMT 3637: "The Contractor shall provide the ability to monitor security---related devices for failures in the equipment."

[105] Project Requirements relevant to Security Operators being able to access Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass FAT include those requiring the contractor to provide:

1) "Alarm Management that is capable of providing a drill---down function when requested for each aggregated alarm (e.g., by priority, by location, by state, by C3 center, by type)(RQMT 2582.1)";

2) "the capability to associate Alarm, Alert and Notification with a particular user" (RQMT 2542);

3) "that in the event routing information indicates that a particular user type is to be alerted upon the occurrence of Alarm, Alert and Notification, then the message is be displayed on each user's appropriate alarm display, wherever each user is currently stationed, including a remote console" (RQMT 2553);

4) "Alarm Management that is capable of providing a drill---down function when requested for only locations or equipment with active alarms"(RQMT 2584);

5) "the filtering ability specified in the previous requirement be available in a real---time fashion via an interface on the alarm display(s)" (RQMT 2585);

6) "Alarm Management that logs all newly generated C2 Alarms, Alerts and Notifications to a database" (RQMT 2608);

7) that "the ID of the Alarm is logged to the database" (RQMT 2615.2);

8) that "at minimum, the following information shall be logged: identification of the person making the change (logon information), what was changed (field name), old value, new value, the date and the time of the change and whether this change was an override of automatically entered information" (RQMT 2628);

9) "a Reporting capability that allows authorized C2 Users to transfer deposited voice files to the database" (RQMT 2761);

10) "a Reporting capability to allow authorized C2 Users to provide beginning and ending pointers and the name of the master voice recording file(s) (e.g., from either of the voice playback functionality or to be accessible from other systems voice storage)" (RQMT 2766);

11) "that whenever an extracted voice clip is linked to a report, the report shall provide the beginning and ending pointers and the name of the master voice recording file(s) that the clip was extracted from, specifying a link back to the original recording." (RQMT 2768);

12) that "all data, other than digital CCTV video and voice communication data, managed by all C3 centers shall remain available on---line for at least 30 days, whereupon it shall then be archived" (RQMT 2770);

13) "simulation that automatically starts in a clear (un---initialized) state upon valid logon and entry into the Maintenance modes" (RQMT 2877);

14) "a workstation that is automatically configured as defined by the scenario, if provided, upon log---on as a Trainee" (RQMT 2903);

15) that "an authorized C2 User operating a workstation as a Maintainer can control, in real time, the simulation" (RQMT 2908);

16) that "the Maintainer can dynamically inject all possible incident conditions in order to modify the behavior of the system" (RQMT 2909);

17) that "the Maintainer can remotely access a workstation such that the Maintainer can work concurrently with a server and a workstation or with two (2) workstations" (RQMT 2910);

18) that the "Maintainer can interact with the Simulator to modify field responses, modify parameters, induce operator errors and inject simulator outputs" (RQMT 2911);

19) that the "Maintainer can dynamically modify Simulator parameters during scenario creation or execution of a simulation session." (RQMT 2912);

20) "that allows logging and cataloging of individual archived video footage with relevant identifications such as but not limited to date, time, period, location of camera, facility, incident information, archival period, archive expiration date, medium identification, storage location, etc." (RQMT 3496); and

21) "DVRD software functionality that includes retrieval wizard such that an authorized C2 User shall be able to easily and quickly retrieve video archived to removable digital media" (RQMT 3516).

Project Requirements relevant to Security Operators being able to access Security Information as required that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" and that did not pass MTAPD SIST include those requiring the contractor to provide:

1) that "the settings for one camera shall not affect the settings of another camera" (RQMT 14784);

2) "Post---Event Forensic Investigation that collects performance data for scenarios to run as training exercises or as real life responses to emergency situations" (RQMT2029);

3) "a Resource Management capability that is available only to authorized C2 Users" (RQMT 2049.2);

4) "an Asset Catalog that includes MTA and Agency personnel (e.g., NYPD Transit Police, MTA Police, Agency maintenance crews), emergency response personnel (e.g., EMS and NYPD), equipment (e.g., tow trucks and maintenance transit vehicles), devices (e.g., CCTV cameras and CIS signs) and expendable resources (e.g., gasoline) (RQMT 2054);

5) specificity as to the "specify the set of security/emergency response resources of all the applicable Agencies, within the Asset Catalog" (RQMT 2057);

6) "Resource Management that provides a capability to interface with Agency systems that provide updated asset and resource data, as determined during design" (RQMT 2075);

7) "a Command and Control System that provides software functions and GUI for local and remote locations, via the network, setup and control of parameters governing the recording, and playback of CCTV images processed by all DVRDs" (RQMT 2132.1);

8) "a Response Execution Display that provides to the authorized C2 User, the ability to drill down to associated information (e.g., Video feeds)" (RQMT 2176);

9) "Alarm Management that is capable of providing a drill---down function when requested for each aggregated alarm (e.g., by priority, by location, by state, by C3 center, by type)" (RQMT 2582.2);

10) "Alarm Management that is capable of providing a drill---down function when requested for each aggregated sensor data set (sensor, stored video, network intrusion detection, access control)" (RQMT 2583); and

11) "different Command and Control System data to be defined for each C3 Center." (RQMT 3045).

Project Requirements relevant to Security Operators being able to access Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass B&T SIST include those requiring the contractor to provide:

1) "Execution Management that identifies to an authorized C2 User, any lack of information being received, gaps in the information or conflicting information and can highlight missing or conflicting information" (RQMT 2004);

2) "Alarm Management that is capable of providing a drill---down function when requested for each aggregated alarm (e.g., by priority, by location, by state, by C3 center, by type)" (RQMT 2582.2);

3) "Alarm Management that is capable of providing a drill---down function when requested for each aggregated sensor data set (sensor, stored video, network intrusion detection, access control)" (RQMT 2583); and

4) "a centralized administration tool for C2 User defined profiles, restricting C2 User's security access to specific video/audio channel and/or to a specific system operation, such as video monitoring and playback and or setup" (RQMT 3509).

106 Project Requirements relevant to Security Operators managing Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass FAT include those requiring the contractor to provide:

1) "a window to alert C3 Center maintenance personnel to an event, and allow them to acknowledge and otherwise track an event report" (RQMT 2420);

2) "Alarm Management that provides a centralized interface --- a uniform clearinghouse --- for all Security---related Alarms, Alerts and Notifications" (RQMT 2517);

3) "Alarm Management that provides the functionality to allow authorized C2 Users to define the 'priority' of each Alarm, Alert and Notification message" (RQMT 2534);

4) "Alarm Management that provides the functionality to allow authorized C2 Users to define the 'states' of each Alarm, Alert and Notification message" (RQMT 2536);

5) "an alarm display that provides a centralized clearinghouse for any and all alarms (including alarms that are monitored by the IESS)" (RQMT 2580);

6) "different audio and visual warning indications to permit the user to quickly determine the criticality and location of the Alarm, Alert and Notification" (RQMT 2640); and

7) "Emergency Situation Notification that has two parts: first, is the creation and maintenance of a list of personnel to notify in case of an Emergency Situation and applicable procedures to follow; and second, is the creation and maintenance of information regarding emergency situation that is stored in a database that can be selectively queried for information retrieval, maintained by authorized users and allow for on screen display and printing of information" (RQMT 2645).

Project Requirements relevant to Security Operators managing Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass MTAPD SIST include those requiring the contractor to provide:

1) "a system, which funnels Alerts/Alarms upwards according to the business rules and the Decision Support Subsystem" (RQMT 1850);

2) "a Command and Control System with all of the C2 functionality at all of the C3 Centers, but the functionality at each C3 Center is data and business rule driven" (RQMT 1899);

3) "a system that, when in Emergency Mode, provides all the capability of Normal Mode and adds functionality to assess security incidents or potential security incidents that might adversely affect MTA operations, employees, or passengers and provide Incident Management/Decision Support capability" (RQMT 1902);

4) "the capability for an authorized C2 User to initiate a change of the Mode of Operation to Emergency Mode when a security event (e.g., Incident or Emergency Situation) occurs, only when the C3 Center is in Operational status and in Normal Mode" (RQMT 1909);

5) "Incident Management/Decision Support that allows C2 Users to initiate the generation and execution of a Response Plan in response to a security event" (RQMT 1929);

6) "a Common Operational Picture that provides, to the authorized C2 User, an integrated presentation of Station Overlays" (RQMT 2153);

7) "Asset and Resource Displays that provide the authorized C2 Users with the capability to update any automatically entered asset and resource data" (RQMT 2180);

8) "each authorized C2 User the ability to track a maintenance event from the time of its occurrence to its conclusion" (RQMT 2419);

9) "a system that automatically enters all known data about the maintenance event as it is reported" (RQMT 2424);

10) "the capability for an authorized C2 User to place the C3 Center into Maintenance Mode, when the C3 Center is being upgraded or repaired" (RQMT 2875);

11) "the capability for an authorized C2 User to place the C3 Center into Normal Mode, when the upgrade or repair is completed" (RQMT 3395.2);
12) a system that gives "each C2 User the ability to sort the telephone directory by selecting one or more of the key fields listed above" (RQMT 2876);

13) a system that allows "each VLR to be able to continuously archive recorded audio on removable digital media including, but not limited to, Compact Disk---Read Write (CD---RW) and DVD---RAM, for a minimum of 30 days before human intervention is required to exchange media" (RQMT 3442);

14) "a NMS that includes the ability to identify trends and determine how to optimize the network by changing configurations or replacing network devices" (RQMT 3615); and

15) that "[t]he maintenance schedule for each device, for which maintenance is recommended by the manufacturer, shall be programmed" (RQMT 14919).

Project Requirements relevant to Security Operators managing Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass B&T SIST include those requiring the contractor to provide:

1) "the capability for an authorized C2 User to place the C3 Center into Normal Mode, when the upgrade or repair is completed" (RQMT 2876);

2) "a Command and Control System that provides software functions and GUI for local and remote locations, via the network, setup and control of parameters governing the recording, and playback of CCTV images processed by all DVRDs" (RQMT 2132.1);

3) "a Command and Control System with a default set of business rules, which will be developed by the Contractor in coordination with the Agencies during the design phase" (RQMT 2280);

4) "a Simulator that simulates the data exchange, messages and failure scenarios in the communication protocol"(RQMT 2891);

5) "Access Control badging stations that shall issue smarts cards, update the database, and perform any necessary maintenance for the Access Control functions" (RQMT 2951);

communicated,[107] or secured[108] as required.

6) "each C2 User the ability to sort the telephone directory by selecting one or more of the key fields listed above" (RQMT 3395.2); and

7) "a VCS with the ability for an authorized C2 User to prioritize incoming telephone calls" (RQMT 3408).

[107] Project Requirements relevant to Security Operators communicating Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass FAT include those requiring the contractor to provide:

1) "Alarm Management that routes Alarm, Alert and Notification to a subscribing agency information system" (RQMT 2557);

2) "Alarm, Alert or Notification that is routed to at least one of the pre---defined list of Alarm, Alert and Notification destination subscribers (i.e., a user or a system)" (RQMT 2558.1);

3) "Emergency Situation Notification that has two parts: first, the creation and maintenance of a list of personnel to notify in case of an Emergency Situation and applicable procedures to follow; and second, the creation and maintenance of information regarding emergency situation that is stored in a database that can be selectively queried for information retrieval, maintained by authorized users and allow for on screen display and printing of information" (RQMT 2645);

4) that "all aspects of C2 System integration including, but not limited to, logon information, group access privileges, alarm information, and electronic telephone directory, shall be included in the interface between the C2 System and the VCS" (RQMT 3342.2);

5) that "the Contractor shall integrate the VCS to include the ability to exchange data handled by the VCS, such as a Call History Report or the MTA Telephone Directory, with other components of the C3 Center" (RQMT 3345);

6) "the ability to download the MTA Telephone Directory, if available in electronic format, into the VCS electronic telephone directory" (RQMT 3390);

7) that "authorized C2 Users are able to create, modify and delete entries within the electronic telephone directory" (RQMT 3397); and

8) "a VCS that supports automatic telephone dialing capability initiated from any electronic form within the C3 Center" (RQMT 3420).

Project Requirements relevant to Security Operators communicating Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass MTAPD SIST include those requiring the contractor to provide:

1) a system that ensures that "external interfaces [referring to portions of systems and/or specific devices outside of the MTA (i.e., non---MTA agencies)] can communicate with the C3 Center over voice, data, and video circuits or via communications gateways" (RQMT 3644);

2) "the voice, FAX, email, CCTV, and data interfaces to local agencies as described below" (RQMT 3704), including "the ability to send/receive CCTV video images to/from NYPD" (RQMT 3709);

3) "the following interfaces between each C3 Center and the New York State Police" (RQMT 3743), including "the ability to send/receive CCTV video images to/from New York State Police" (RQMT 3747);

4) "interfaces between each C3 Center and AMTRAK" (RQMT 3780); and

5) "the ability to send/receive CCTV video images to/from AMTRAK" (RQMT 3784) that "announcements shall include telephone numbers and names of Authority and other service personnel" (RQMT 14920).

Project Requirements relevant to Security Operators communicating Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass B&T SIST include those requiring the contractor to provide:

1) "a C2 System that assists users in notifying the appropriate response agencies, when the system detects a security incident" (RQMT 3636);

2) "external interfaces [referring to portions of systems and/or specific devices outside of the MTA (i.e., non---MTA agencies)] that can communicate with the C3 Center over voice, data, and video circuits or via communications gateways" (RQMT 3644);

3) "the voice, FAX, email, CCTV, and data interfaces to local agencies as described below" (RQMT 3704), including "the ability to send/receive CCTV video images to/from NYPD" (RQMT 3709);

4) "the voice, FAX, pager, email, CCTV, and data interfaces to state agencies as described below" (RQMT 3738), including the "interfaces between each C3 Center and the New York State Police" (RQMT 3743), "the ability to send/receive CCTV video images to/from New York State Police" (RQMT 3747), and "interfaces between each C3 Center and AMTRAK" (RQMT 3780); and

5) "the ability to send/receive CCTV video images to/from AMTRAK" (RQMT 3784).

108 Project Requirements relevant to the Required System securing Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass FAT include those requiring the contractor to provide:

1) "a log-on/log-off function that is an application level log-on/log-off for the user at the particular workstation, and shall not cause any of the application processes to stop or restart except applicable to the workstation where the log-on/log-off occurs" (RQMT 3138.2);

2) "capability for a C3 Center computer system user to transfer control of all, or a portion of, his/her assigned territory to another user having access rights consistent with those being transferred, and subject to the concurrence of both users" (RQMT 3199);

3) capability "where a C3 Center computer system user that is in receipt of the transfer shall be prompted to accept or deny the transfer" (RQMT 3200);

4) "that the System Administrator has the ability to reset, within each C3 Center; the default settings that establish pre-defined function access assignments for each user classification" (RQMT 3222); and

5) "in the set of functions alarms that may be inhibited" (RQMT 3236).

Project Requirements relevant to the Required System securing Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass MTAPD SIST include those requiring the contractor to provide:

1) that "Read and write access to the external server shall be permitted by authorized users only. Authorized users shall be provided a valid username and password to gain access to the external server" (RQMT 2509);

252. Because these requirements were never demonstrated to be functional during Project testing, the only conclusion is that the Lockheed System does not function as required and provides a far lesser level of security than was promised.

B.2.2. "Unwritten Expectation"

253. The Aella/DeStefano Report re-categorizes 57 non-passed requirements under the category "Unwritten Expectation," based on LTD's opinion that "that the requirement was demonstrated, however, MTA representatives expected it to function in a different manner."[109] I am aware of no evidence, and LTD cites no evidence, that the MTA failed such requirements based on expectations not apparent in the plain language of the Contract.

254. Much of what the Aella/DeStefano Report categorizes as "Unwritten Expectation" relates to the Project's requirements that Lockheed integrate various software

2) "user classifications that are supported by Access Management that includes Remote User - monitor only capability" (RQMT 3162); 3) "a C2 System that uses Secure Sockets Layer (SSL) or other encryption method for all web-based communications" (RQMT 3254);

4) a system that ensures that "data identified as 'sensitive data', or any data that is considered data protected by the Privacy Act, is encrypted before being sent via the web" (RQMT 3294);

5) "a database that supports data partitioning by each C3 Center (central, regional and local)" (RQMT 3297); and

6) that "the MS shall provide Resource Access Control including: Levels of access privileges to system MS and NE capabilities, Levels of system commands and information access, Mechanisms for restricting access to partitions of the data" (RQMT 15404).

Project Requirements relevant to the Required System securing Security Information that the Aella/DeStefano Report categorizes as "Functionality Demonstrated" that did not pass B&T SIST include those requiring the contractor to provide:

1) "a C2 System that uses Secure Sockets Layer (SSL) or other encryption method for all web---based communications" (RQMT 3254);
2) a system that ensures that "data identified as 'sensitive data', or any data that is considered data protected by the Privacy Act, is encrypted before being sent via the web" (RQMT 3294); and

3) "an image of the firewall to be available for reloading and restarting the firewall to a working configuration if the firewall is a computer implementation" (RQMT 3576).

[109] Aella/DeStefano Report, page 79.

components into an effective, practical system for Security Operators to use. The Aella/DeStefano Report's application of this unauthorized category is consistent with its incorrect position that a hodge-podge of COTS products with limited "interfaces" (and correspondingly limited functionality) is contractually compliant.

255. For example, there are a series of 15 requirements related to "Information Playback data." One of those requirements, Requirement 2789, states that Information Playback Data shall include "appropriate versions of system databases, software versions, and control data to form a complete and accurate version of the system for the requested Playback time period" [emphasis added]. This requirement refers to data from the computer-aided dispatch, access control, video, and voice systems. According to the testing record,[110] this requirement failed because the Lockheed System could only play back "display data" (i.e., only the data that appeared on the operator's screen) and did not play back the other types of data that were supposed to be captured by the system (i.e., the underlying data from the various subsystems that may not have been displayed on an operator's screen in a given module at a given point in time).

256. The Aella/DeStefano Report categorized these 15 Information Playback requirements as "Unwritten Expectation."[111] Based on the text of the requirements, as well as the testing record, it is clear to me that these requirements failed because the system was unable to do what the requirements stated, not because MTA had an unrealistic expectation of what the requirements meant.

257. Similarly, Requirement 2128 clearly states that "the Contractor shall provide a Command and Control System that facilitates intrusion detection notification that identifies the

[110] See Test Verification and Acceptance Form and Post Test Briefing, both dated June 4, 2008, available on ProjectSolve.

[111] Aella/DeStefano Report, Exhibit A, page 15.

appropriate Agency to notify, the Agency personnel to contact and provides any alarm information concerning the potential intruder, the time of the intrusion and the location of that intrusion." The Aella/DeStefano Report deems this requirement to be met by the system by merely having contact information "available" in Microsoft Exchange, an e-mail program.

258. The Aella/DeStefano Report dismisses MTA's wholly reasonable (and entirely correct) expectation that incident management contact information would be retrievable in the operator's primary incident management module (known as iConsequence), and instead deems this failure to be a "pass" under the "Unwritten Expectation" category.

259. Another set of requirements in the Aella/DeStefano Report's "Unwritten Expectation" category reflects the fact that the Lockheed System does not properly integrate business rules (some of which were never even created) or provide the required decision support to operators.

260. For example, Lockheed's inability to provide and implement business rules to handle multiple alarms or events at all in i/Alarm prevented Lockheed from passing Requirement 2119,[112] yet the Aella/DeStefano Report categorizes this critical shortcoming as "passed," despite the fact that many of the required business rules for which Lockheed was responsible were never even drafted. The MTA's expectation that the required functionality would be accessible to Security Operators in the primary alarm management module, i/Alarm is consistent with the Contract and was wholly reasonable and consistent with standards in the security system industry.

261. Overall, Lockheed's failure to pass the requirements contained in the Aella/DeStefano's "Unwritten Expectation" category results in a system where security operators

[112] "The Contractor shall provide a Command and Control System that performs analysis of alarm information to detect threats, based upon the defined business rules" (RQMT 2119).

may be unaware of non-functioning devices and processes,[113] and where the Security Information that is conceptually available cannot be accessed,[114] managed,[115] communicated,[116]

[113] Project Requirements relevant to making Security Operators aware that a device or process may not be functioning that the Aella/DeStefano Report categorizes as "Unwritten Expectation" that did not pass FAT include those requiring the contractor to provide:

> 1) "a Failure Notification Log that maintains the set of all failure notification messages with associated attribute values (e.g., timestamp, notified person(s))" (RQMT 2465.2);
>
> 2) "a Failure Notification Log that is viewable by authorized C2 Users" (RQMT 2466);
>
> 3) "security to ensure that the Failure Notification Log data cannot be modified or deleted" (RQMT 2467.2); and 4) a system that ensures that "each report contains a Failure Message display area, to notify the user of any user guidance and user entry failures" (RQMT 2477).

Other Project Requirements relevant to making Security Operators aware that a device or process may not be functioning that the Aella/DeStefano Report categorizes as "Unwritten Expectation" include those requiring the contractor to provide:

> 1) "Equipment Trouble Reporting capability that enables equipment trouble data to be entered, retrieved, updated, processed and incorporated into trouble reports" (RQMT 2647, did not pass MTAPD SIST); and
>
> 2) "provide each authorized C2 User the ability to project the graphic diagram, in its entirety, on the other functional projection units in the event of a projection failure" (RQMT 2408, did not pass B&T SIST).

[114] Project Requirements relevant to Security Operators accessing Security Information that the Aella/DeStefano Report categorizes as "Unwritten Expectation" that did not pass FAT include those requiring the contractor to provide:

> 1) "from historical data, Information Playback capability that recreates the conditions and user interactions that were present at the selected Playback time period and subsequent changes that occurred from that point in time on the workstation being used for playback (no dedicated workstations exist for playback - any C3 workstation may be used as for playback)" (RQMT 2785);
>
> 2) "the same display formats for Playback as for actual C3 operations, except that a clear, distinguishing attribute (e.g., a combination of text with a uniquely colored border) is provided to distinguish displays presented during Playback from those presented during actual C3 operations" (RQMT 2786);
>
> 3) "an Information Playback capability that prevents alteration of real-time or existing historical data by the Playback execution or by any user" (RQMT 2787);
>
> 4) "an Information Playback capability that retrieves the Playback data that matches the user-selected date and time period, from historical archives" (RQMT 2788.3);
>
> 5) a system that ensures that "Information Playback data to be retrieved includes the appropriate versions of system databases, software versions, and control data to form a complete and accurate version of the system for the requested Playback time period" (RQMT 2789);
>
> 6) "an Information Playback capability that prevents authorized C2 Users from issuing any device control commands or modifying the state of the real-time operational system during a playback session" (RQMT 2790);

7) "an Information Playback capability that provides authorized C2 Users the ability to control the playback session, including stop" (RQMT 2791), "start" (RQMT 2792), "pause" (RQMT 2793), "resume" (RQMT 2794), and "terminate playback" (RQMT 2795), and "that processes user requests to start, stop, pause, resume and terminate the Playback session" (RQMT 2796);

8) that "shall suspend playback processing, while Playback is in pause mode, until the user requests that the session resumes or the user terminates the session completely" (RQMT 2797); and

9) "an Information Playback capability that allows authorized C2 Users to terminate a playback session at any point during playback" (RQMT 2799).

Likewise, in relation to the ability of Security Operators to access Security Information as required, the Aella/DeStefano Report categorizes RQMT 2306, which did not pass MTAPD SIST, as "Unwritten Expectation." RQMT 2306 requires that "The Contractor shall create a single library of icons, consistent with the operational needs of each Agency."

115 Project Requirements relevant to Security Operators managing Security Information that the Aella/DeStefano Report categorizes as "Unwritten Expectation" that did not pass FAT include those requiring the contractor to provide:

1) "the capability to enter High-Level Objectives in a pre-defined format that includes an action and a location" (RQMT 1946);

2) "Resource Management with data entry screens for adding and deleting to the set of static and dynamic resource information available for emergencies" (RQMT 2068);
3) "a Command and Control System that performs analysis of alarm information to detect threats, based upon the defined business rules" (RQMT 2117);

4) "the capability for an authorized C2 User to initiate a re-analysis based upon the new security alarm information" (RQMT 2118);

5) "a Command and Control System that generates an alarm message based upon the analysis of alarm information that detects aggregated alarms or inferred alarms" (RQMT 2119);

6) "a list of all extracted video files to be presented, in reverse chronological order or by type of file (presentation format to be user selectable), for linking to accidents, observations, incidents" (RQMT 2768);

7) a system that ensures that "the System Administrator has the ability to add, delete or edit the set of High-Level Objectives (containing an action and a location), within each C3 Center" (RQMT 3005);

8) a system that ensures that a "System Administrator is able to view and edit the rules used for analysis of the security alarm information" (RQMT 3020.2);

9) that "the rules for analysis of the security alarm information can be edited in such a way as to allow for the addition/deletion or modification of the data/rules/models used in support of the information analysis (e.g., a rule-based editor or changes to parameters/thresholds in a model)" (RQMT 3021);

10) that "the System Administrator is able to modify the set of security events and the list of actions in response to the security event" (RQMT 3022);

11) a system that includes "Playback in the set of functions for Report Management" (RQMT 3247); and

12) a system that includes "Territory Assignment control in the set of functions for Report Management" (RQMT 3250).

Project Requirements relevant to Security Operators managing Security Information that the Aella/DeStefano Report categorizes as "Unwritten Expectation" that did not pass MTAPD SIST include those requiring the contractor to provide:

> 1) "the capability for an authorized C2 User to initiate a change of the Mode of Operation to Normal Mode when the security event is closed, only when the C3 Center is in Operational status (the C3 Center is operational - running and functioning as a C3 Center) and in Emergency Mode" (RQMT 1913);
>
> 2) "Incident Management/Decision Support that allows C2 Users to initiate the generation and execution of a Response Plan in response to a security event" (RQMT 1929);
>
> 3) "a Response Plan capability that can be further refined using functionality to predict and assess the consequences of the task propagation" (RQMT 1970);
>
> 4) "Execution Management capability that continually evaluates how well the current Response Plan is addressing the incidents/emergency situations" (RQMT 2001);
>
> 5) "Execution Management with the capability to change the Operational Mode, as warranted by the increase or decrease in severity and scope of the event" (RQMT 2003);
>
> 6) "a system that provides data entry fields for manual entry of severity level of the event, the specific location where the event has taken place, person(s) performing the maienance activity, whether or not the event is scheduled maintenance, a full-text explanation of the maintenance event, a quick explanation or a standard set of keywords that achieves brevity in explanation and provides a consistent search target for database queries, spare parts or other materials used, and the amount of labor in man-hours for all maintenance events" (RQMT 2426);
>
> 7) "conditions for generation of Alarms, Alerts and Notifications that include any and all characteristics of the Alarm, Alert and Notification, for example, threshold tolerances that dictate when a particular Alarm, Alert and Notification is triggered" (RQMT 2529);
>
> 8) "override of any report control parameter value that is logged, including the date and time, the user who performed the override, the default value and the value as changed" (RQMT 2687);
>
> 9) "a NMS that communicates in an open fashion with asset management software which will keep track of maintenance records, replacement records, maintenance cost records and handle the automatic dispatch of maintenance crews via email and pager" (RQMT 3594);
>
> 10) "a NMS that generates alarms, display, and logs them in the C2 System for incorporation into the Alarm Management Subsystem, for all performance parameters that are outside of configurable threshold values" (RQMT 3607); and
>
> 11) "at the MCV console position the same functionality that is available at the Central C3 Center consoles for multimedia information management, for example, the users may transfer digital photograph files taken at the remote site to the database" (RQMT 3607).

Project Requirements relevant to Security Operators managing Security Information that the Aella/DeStefano Report categorizes as "Unwritten Expectation" that did not pass B&T SIST include those requiring the contractor to provide:

> 1) "Alarm Management that provides the functionality to permit authorized C2 Users to view the log of Alarm, Alert and Notification message changes" (RQMT 2623); and

or secured[117] as required.

B.2.3. "COTS Program Restriction/Limitation"

262. The Aella/DeStefano Report re-categorizes 28 requirements that did not pass FAT

2) "a NMS that communicates in an open fashion with asset management software which will keep track of maintenance records, replacement records, maintenance cost records and handle the automatic dispatch of maintenance crews via email and pager" (RQMT 3594).

[116] 47 Project Requirements relevant to Security Operators communicating Security Information that the Aella/DeStefano Report categorizes as "Unwritten Expectation" that did not pass FAT include those requiring the contractor to provide:

1) "a Command and Control System that facilitates intrusion detection notification that identifies the appropriate Agency to notify, the Agency personnel to contact and provides any alarm information concerning the potential intruder, the time of the intrusion and the location of that intrusion"(RQMT 2128.1: RQMT 2128.2);

2) "the ability for the authorized C2 User to quickly determine the person to contact in each Agency, based upon the type of Incident/Emergency Situation, the day of the week and the time of day and provide their contact information" (RQMT 2492); and

3) "a system that provides the ability for each authorized C2 User to contact a pre-specified list of emergency response personnel at each Agency, based upon the type of Incident/Emergency Situation, the day of the week and the time of day" (RQMT 2502).

Project Requirements relevant to Security Operators communicating Security Information that the Aella/DeStefano Report categorizes as "Unwritten Expectation" that did not pass MTAPD SIST include those requiring the contractor to provide:

1) "a Reporting capability that provides, to authorized C2 Users, a commercially available name and contact information (e.g., work phone numbers, pagers, mobile phone numbers) capability that is delivered containing the most recent complete list of MTA and agency employees, their e-mail addresses and their work mailing addresses" (RQMT 2965);

2) "for transferring the connection of various voice communication systems between any of the user positions in a given C3 Center, and between users at one C3 Center to another C3 Center" (RQMT 3356.2);

3) "VCS forms that include a telephone call history form displaying incoming calls, outgoing calls, answered calls, unanswered calls, date, time, and caller ID that the C2 User can scroll, search, and redial a selected entry" (RQMT 3406) (also did not pass B&T SIST); and 4) "a VCS with the ability for an authorized C2 User to prioritize incoming telephone calls" (RQMT 3408).

[117] Project Requirements relevant to the Required System securing Security Information that the Aella/DeStefano Report categorizes as "Unwritten Expectation" that did not pass MTAPD SIST include those requiring the contractor to provide:

1) "password assignments for network administrator accounts on firewall systems according to standards of secure password selection as recommended by Request For Comments (RFC) standards including, but not limited to, 2289 (STD-061), 2444, 3370, etc." (RQMT 3578); and

2) a "secure password generator for general use in the C3 Center or the Contractor may deliver this tool as a built-in from one of the delivered Operating System suites" (RQMT 3580).

as "deferred" under the category "COTS Program Restrictions/Limitation," based on LTD's opinion that "the approved COTS product did not meet the functional requirement."[118]

263. As detailed in Section II above, Lockheed agreed to meet 100% of the requirements of the project. Lockheed's inability to do so based on the COTS products that it selected for the system architecture does not relieve Lockheed of its obligation to deliver the Required System.

264. The Aella/DeStefano Report's arguments to the contrary are merely excuses that unconvincingly attempt to deflect blame from Lockheed to third parties that Lockheed selected, for a system that Lockheed was responsible for designing and delivering.

265. In the security industry, it is understood that a contractor's solution is required to meet the requirements of a contract regardless of whether the COTS products that the contractor picks are able to meet all of the contract's requirements on their own. Lockheed's failure to pass these requirements results in a system where user- entered data cannot be validated as required,[119] security operators may be unaware of non-functioning security devices and/or

[118] The Aella/DeStefano Report considered a requirement in this category "Deferred" if a Contract Waiver Request (CWR) was granted and "Failed" if no CWR was granted.

[119] Project Requirements relevant to data validation that the Aella/DeStefano Report categorizes as "COTS Program Restriction/Limitation" that did not pass FAT include those requiring the contractor to provide:

> 1) "a Command and Control System where all user-entered data is validated for reasonableness of content" (RQMT 2281.1, RQMT 2281.3 & RQMT 2281.4);
>
> 2) "a Command and Control System where data validations include intra-field and inter-field validations" (RQMT 2282.1, RQMT 2282.3 and RQMT 2281.4);
>
> 3) "a Command and Control System where input data is checked at the source of data entry, in order to ensure prompt and proper correction of the data by the person entering the data" (RQMT 2283.1, RQMT 2283,3 and RQMT 2281.4);
>
> 4) that "the Command and Control System shall detect and report invalid entries to the user via an error message" (RQMT 2301);
>
> 5) "a Command and Control System that does not require acknowledgement of error messages" (RQMT 2303);

processes,[120] and security information cannot be accessed,[121] managed,[122] or secured[123] as

6),a system that ensures "where manually entered data is invalid, that the entry form shall revert back to the last valid entry for the field" (RQMT 2626);

7) "a Reporting capability that contains a commercially available Spelling Help function that presents options of correctly spelled words based upon the user's attempt at spelling a word and once the user chooses the correct spelling, enters it into the text" (RQMT 2963); and

8) "a Spelling Help function that has the ability to spell check a single word or blocks of text, as specified by the user" (RQMT 2964).

[120] See Requirement 3066.2 ("The Contractor shall provide a Failure Handling Log that contains the set of all failure messages.")

[121] Project Requirements relevant to Security Operators accessing Security Information that the Aella/DeStefano Report categorizes as "COTS Program Restriction/Limitation" that did not pass FAT include those requiring the contractor to provide:

1) a system that ensures "that an acknowledged Alarm, Alert and Notification remains on a user's display until the end of the shift, at which time the Alarm, Alert and Notification message shall be retired" (RQMT 2567);

2) "the capability for text and portions of text appearing in a window to be assigned a different size for each specific application without recoding the application (i.e., such customization shall be available through user configuration settings)" (RQMT 2286);

3) "an Employee Information function that provides an authorized C2 User the ability to locate an Employee's on-line information based upon entry of their name (whole or partial) or their employee number" (RQMT 2944.2); and

4) a "pop-up message" that "shall notify both the higher and lower priority users of the pre- emption" (RQMT 14836).

[122] Project Requirements relevant to Security Operators managing Security Information that the Aella/DeStefano Report categorizes as "COTS Program Restriction/Limitation" that did not pass FAT include those requiring the contractor to provide:

1) "Resource Logging that can be enabled or disabled by a System Administrator" (RQMT 2091);

2) "a Command and Control System that provides a capability for authorized C2 Users to add/delete and modify the information that is obtained from sensors and equipment within the field" (RQMT 3041); and

3) that for the "ability to independently setup each camera for frame rate, compression rate, brightness, contrast and other performance setups" that "these options to be updatable during system operation without interfering with other system operation such as recording and playback" (RQMT 3507, RQMT 3508).

[123] Project Requirements relevant to the Required System securing Security Information that the Aella/DeStefano Report categorizes as "COTS Program Restriction/Limitation" that did not pass FAT include those requiring the contractor to provide:

required.

B.2.4. "Conflicting Specification"

266. The Aella/DeStefano Report re-categorizes nine requirements that did not pass FAT as "deferred" under the category "Conflicting Specification," based on LTD's opinion that each represented "a requirement that conflicted with another specification requirement."[124]

267. In my opinion, categorizing these requirements as "deferred" is inappropriate. These requirements were tested and Lockheed failed to demonstrate the required functionality. Many of these requirements were not mutually exclusive with — and therefore did not "conflict" in whole or in part with — other technical specifications or functionality. Accordingly, when Contract Waiver Requests ("CWRs") were submitted by Lockheed to MTA, they were generally rejected.[125]

268. For example, the Aella/DeStefano Report's assertion that Requirements 2568 and

1) "Access Management that provides the ability for a user to perform a concurrent log- on/log-off (of their workstation) as part of a shift change, where a valid user log-on automatically logs-off the previous user" (RQMT 3146);

2) a system that ensures that "at least one C2 User is logged onto any C3 Center computer system at all times - logout is rejected if this condition is not met" (RQMT 3150);

3) "Access Management that rejects logout requests that would result in a territory being uncontrolled" (RQMT 3186);

4) "Access Management that rejects software lock requests that would result in a territory being uncontrolled" (RQMT 3187);

5) a system that ensures that when access rights are being transferred that "if the receiving C3 Center computer system user accepts, then control shall be immediately transferred from the sending user to the receiving user" (RQMT 3201); and

6) "if the C3 Center computer system user denies the transfer, the control shall remain with the requester and the requester shall receive an advisory message to that effect" (RQMT 3202).

[124] The Aella/DeStefano Report considers 9 of 10 "Conflicting Specification" requirements as "deferred" based on a Contract Waiver Request ("CWR") and 1 as "failed" where no CWR was granted. See page 81 of Aella/DeStefano Report.

[125] CWRs for RQMTs 3203, 3225.1, 3507, 14777, and 14787 were all rejected and CWRs for RQMTs 3098 and 14782 were not approved at the time of Termination.

2597 are in conflict is simply incorrect. Requirement 2568 requires that "active (i.e., unacknowledged) Alarms, Alerts and Notifications have precedence on the display over acknowledged Alarms, Alerts and Notifications Requirement 2597 allows "authorized C2 User to sort the appearance of the alarms on alarm display(s) based on state (i.e., acknowledged/unacknowledged), priority, type, state, or date and time").

269. In other words, the Required System allows users to sort the appearance of alarms on the display while having the unacknowledged Alarms, Alerts and Notifications be displayed in a position of precedence.

270. As another example, Lockheed's failure to meet Requirement 3178, which provides that territories should be available to a computer user based on the "title that they possess, not the physical console where they happen to sit" is not in conflict with nor excused by Requirement 3203 (which prevents a territory from being assigned to a workstation "unless that territory is assigned to the C3 Center").

271. Contrary to the arguments of the Aella/DeStefano Report, these requirements are neither conflicting by their plain language, mutually exclusive in the context of system design nor in the practicality of how individual users are required to operate the Required System.[126]

272. Just because one requirement specifies a procedure whereby individual workstations (computers) can be used to access certain functionality (in this case, manage a territory as per RQMT 3203), does not mean that when an individual sits down to use that workstation, that the computer should lack required functionality based on the user's title (RQMT 3178).

273. As a third example, the existence of the MPEG4 standard as a video compression

[126] See Aella/DeStefano Report, Appendix A at 27 purporting that RQMT 3203 creates a "workstation- specific approach [that] runs counter to the overall interdependency and support design of the redundant C3 centers network."

alternative allowed by Requirement 14776 does not make it impossible to provide the ability to "independently setup each camera for frame rate, compression rate, brightness, contrast and other performance setups" as per Requirement 3507. In other words, just because Lockheed chose video encoders that "do not permit independent control of bandwidth, frame rate and resolution" (see Aella/DeStefano Report, Appendix A), the Required System still could have and is required to have the ability to adjust the speed (rate), quality (compression), and image attributes (brightness and contrast) of the individual cameras (effectively managing and balancing the quantity of data that would be entering the network with the required quality of each image).

274. In sum, the requirements identified by the Aella/DeStefano Report as "Conflicting Specifications" are not in conflict with other contract requirements. These requirements could have, and should have, been met by the Required System. Lockheed's failure to pass this particular subset of requirements results in a system where Security Information cannot be managed[127] or secured[128] as required.

[127] Project Requirements relevant to the Required System managing Security Information that the Aella/DeStefano Report categorizes as "Conflicting Specification" that did not pass FAT include those requiring the contractor to provide:

1) that "active (i.e., unacknowledged) Alarms, Alerts and Notifications have precedence on the display over acknowledged Alarms, Alerts and Notifications" (RQMT 2568);

2) "the ability to independently setup each camera for frame rate, compression rate, brightness, contrast and other performance setups" (RQMT 3836);

3) that "the frame rate, resolution and bandwidth shall be individually adjustable" (14777);

4) that "for each camera, the recorded frame rate shall be adjustable from 1 to 30 frames per second, the resolution shall be adjustable to CIF, 2D or 4CIF; and the recorded bandwidth shall be adjustable" (RQMT 14782); and

5) that "the settings (e.g., frame-rate, resolution) of the recorded and real-time digital video shall be independent of each other" (RQMT 14787).

B.2.5. "Demonstrated at Dry Run"

275. The Aella/DeStefano Report re-categorizes five requirements that did not pass FAT as "passed" under the category "Demonstrated at Dry Run," based on LTD's opinion that each "was successfully demonstrated and witnessed by the CA [Commissioning Agent] and a MTA representative during the dry run."[129] This argument runs counter to the TEMP and the Contract, both of which specified that Lockheed would have formal testing, not just a dry run, witnessed by MTA and the Commissioning Agent.

276. Further, it is standard in the business of designing, developing and installing software-based security systems for the contractor to verify that requirements are being satisfied via formal "run for the record" (RFR) tests – not practice or "dry runs."

277. The Aella/DeStefano Report's incorrect argument would obviate the need to have formal RFR testing at all. Furthermore, the argument relies on unsubstantiated insinuations that the individual agencies could and did "influence the CA to fail tests which had been accepted in a preceding dry run."[130] These requirements cannot be counted as "pass" where they were not formally tested and passed.

[128] Project Requirements relevant to the Required System securing Security Information that the Aella/DeStefano Report categorizes as "Conflicting Specification" that did not pass FAT include those requiring the contractor to provide:

> 1) "a Security Audit capability that does not provide a means for modifying audit log records or deleting them" (RQMT 3098);
>
> 2) "Access Management that issues an alarm if changing territory selections for a user will leave a section(s) of territory unmonitored" (RQMT 3188);
>
> 3) "Territory Transfer enforces that a territory cannot be assigned to a workstation, within a C3 Center, unless that territory is also assigned to the C3 Center"(RQMT 3478);
>
> 4) "the C2 User the ability to set the function access assignments for a given workstation to one or more of the function access assignments set for its C3 Center" (RQMT 3225.1 and RQMT 3225.2).

[129] Aella/DeStefano Report at 80.

[130] Aella/DeStefano Report at 40.

278. Lockheed's failure to pass this particular subset of requirements results in a system where Security Information cannot be managed as required.[131]

B.2.6. "N/A for FAT"

279. The Aella/DeStefano Report re-categorizes requirements that did not pass FAT as "N/A for FAT" based on its endorsement of unauthorized categories that Lockheed created during testing, such as "A&I" (analysis and inspection), "Delete Suffixes," or "Move to SIST."[132] In doing so, the Aella/DeStefano Report contends that MTA overstates the number and percentage of FAT requirements that did not pass.

280. Regardless of what stage of testing or in which category requirements properly belong, in the case of the Aella/DeStefano Report's "N/A for FAT" none of the requirements classified in this category were ever successfully tested in any other stage of testing during the IESS/C3 Project, and therefore cannot be counted toward any testing pass rate.

[131] Project Requirements relevant to the Required System managing Security Information that the Aella/DeStefano Report categorizes as "Demonstrated at Dry Run" that did not pass FAT include those requiring the contractor to provide:

> 1) "a Resource Log or a historical record of all changes to asset and resource information, all Response Plans, changes made to plans, all events entered and all alarms and messages displayed to all C2 Users" (RQMT 2090.1);
>
> 2) "a Configuration Editor that is capable of specifying (e.g., tabling) each and every possible device state for those physical devices they represent" (RQMT 2363);
>
> 3) "a Reporting capability that allows authorized C2 Users to transfer deposited digital photograph files to the database" (RQMT 2723);
>
> 4) "a Reporting capability that allows authorized C2 Users to transfer sketch files to the database" (RQMT 2737); and
>
> 5) "a Reporting capability that allows authorized C2 Users to transfer deposited digital video files to the database" (RQMT 2751).

[132] Aella/DeStefano Report at 73.

C. The Importance of the Technical Requirements That The Aella/DeStefano Report Admits Lockheed Failed or Otherwise Did Not Pass

281. The first part of this declaration compared the Lockheed System to the Required System based on the requirements that Lockheed failed or otherwise did not pass, as reflected in the project testing record. That analysis showed significant deficits in functionality, usability, and security of the Lockheed System that demonstrated to me that the Lockheed System does not support security operations in a manner even reasonably close to what is required by the Contract. This section of the declaration addresses the subset of those requirements that the Aella/DeStefano Report agrees failed to pass FAT and/or SIST.

282. The Aella/DeStefano Report admits that 89 of the 315 documented non-passed requirements in FAT and 24 of the 543 non-passed requirements in the partially- conducted SIST testing[133] failed testing (the "Admitted Non-Passed Requirements"). In separate sections analyzing FAT and MTAPD and B&T SIST, the Aella/DeStefano Report states that "none" of the Admitted Non-Passed Requirements should have been considered "Severity 1 or 2" and that the ones that did not have a "workaround" did not "impact critical functions or relate to a system problem that results in significant degradation of major operational functions or performance/stability."[134]

283. In my opinion, these conclusions in the Aella/DeStefano Report are incorrect. These requirements, which indisputable failed tests and/or which Lockheed indisputably refused or was unable to successfully test, were fundamental to the Required System and the absence of these requirements in the Lockheed System has a major impact on functionality and usability of

[133] See Appendix 1, Page 67 of "EXPERT REPORT: DEFICIENCIES IN THE IESS/C3 PROJECT AND THE COST OF REMEDIATION" by Howard Reith of Dnutch Associates, which specifies the number of requirements that did not pass SIST testing at various locations.

[134] See Aella/DeStefano Report at 84.

the system the MTA was left with and must now use.

284. Sections C.1 through C.7 below specifically address the Admitted Non-Passed Requirements and demonstrate that the Lockheed System's failure to pass these requirements renders the Lockheed System significantly less effective in protecting MTA Assets than the Required System would have been, notwithstanding the Aella/DeStefano Report's sweeping and inaccurate dismissal of the importance of the Admitted Non-Passed Requirements.

285. In examining the significance of the Admitted Non---Passed Requirements, I applied the same categories that I used in my Initial Expert Report when examining the larger subset of project requirements that Lockheed did not pass:

- Lack of Awareness of Security Information: Security Operators are left unaware of certain alarms, alerts, notifications, and other critical data;

- Unreliability of Security Information: Security Operators are unable to rely on the Security Information that they receive;

- Lack of Understanding of Security Information: Security Operators lack required tools and training to sufficiently understand the limited Security Information that they receive;

- Inability to Manage & Communicate Security Information: Security Operators lack required tools to help manage and communicate the limited Security Information that they receive;

- Inflexibility: Security Operators are unable to enter and interact with the limited Security Information that they receive in a flexible manner;

- Insecure Security Information: Security Operators are forced to use a system that does not properly secure Security Information; and

- Inefficiency: Security Operators are forced to use a system that is cumbersome and inefficient to operate.

C.1. Lack of Awareness of Security Information

286. With regard to the subset of Admitted Non---Passed Requirements analyzed in this section, the Lockheed System creates situations in which a Security Operator is not made

aware of, and therefore cannot react to, a security event or incident because:

- Certain security devices do not deliver Security Information to a Security Operator as required;[135]

- When security devices in the field are not functioning, the system does not report to Security Operators that such devices are not functioning, as required;[136] and

- Security Operators cannot access Security Information as required.[137]

287. The potential, direct, and dangerous impact of Security Operators being unaware of Security Information is that they cannot act to effectively detect and respond to a security event. Consequently, more people may be killed or injured, more property may be damaged, and MTA operations may be interrupted for longer periods of time than if Security Operators were properly apprised of Security Information as mandated by the Required System.

[135] RQMT 40.2 ("Computer analytics shall also be deployed for artificial intelligence that will generate alarms for anomalies such as abandoned packages and motion detection (Broadware)"); RQMT 2353 ("The Contractor shall provide a Configuration Editor that supports the creation of graphic diagrams using the world coordinate system"); RQMT 2357 ("The Contractor shall ensure global modification of an icon attribute will cause an update to all occurrences of the icon within all graphic diagrams"); RQMT 2374 ("The Contractor shall ensure each occurrence of an icon on the graphic diagram be categorized as Inhibit --- This icon shall serve to indicate when certain of the other functions and attributes assigned to an icon may be inhibited due to internal logic checks or by user selection, in order to inhibit the display of intrusion alarms, for example"); RQMT 2375 ("The Contractor shall ensure each occurrence of an icon on the graphic diagram be categorized as Request in Progress --- This icon shall indicate that a user's request is being acted upon, but is not yet complete"); RQMT 2627.1 ("The Contractor shall ensure all changes to database information are logged and archived"); RQMT 2777 ("The Contractor shall ensure response times for playback, reporting, and querying historical data does not differ from the response times for these same functions done on the 30---day on---line data, once the archived data is loaded and available for playback, reporting, and querying"); RQMT 2778 ("The Contractor shall ensure historic data is subject to full querying and reporting requirements, once the target data is loaded").

[136] RQMT 2361 ("The Contractor shall ensure text fields may change, based upon the state of the device the icon is representing") and RQMT 3522 ("The Contractor shall provide a pop---up alarm as the top window on the authorized C2 User's workstation when one of the elements fails").

[137] RQMT 2291.3 ("The Contractor shall program function keys for quick access to critical, key functions"); RQMT 3223 ("The Contractor shall provide the C2 User the ability to establish function access assignments for the C3 Center"); RQMT 3343 ("The Contractor shall provide a VCS that has an interface to the C2 System for incorporation into the Alarm Management Subsystem"); RQMT 3344 ("The Contractor shall provide all alarm conditions within the VCS that are communicated to the C2 System to be displayed and logged"); RQMT 3485 ("The Contractor shall provide real---time DVRD software capable of searching video sequences for motion in specific image areas"); RQMT 3489 ("The Contractor shall provide real---time DVRD software capable of synchronized playback --- play up to four (4) events with overlapping time synchronized"); RQMT 3514 ("The Contractor shall allow for all cameras belonging to the same group to be set at once"); RQMT 3517 ("The Contractor shall provide auditing and tracking of C2 User activity, and maintenance performed for each DVRD"); RQMT 3522 ("The Contractor shall provide a pop---up alarm as the top window on the authorized C2 User's workstation when one of the elements fails").

C.2. Unreliability of Security Information

288. With regard to the subset of Admitted Non-Passed Requirements analyzed in this section, the Lockheed System creates situations in which a Security Operator cannot rely on Security Information (and would be better able to rely on Security Information under the Required System) because:

- User-entered Security Information is not validated as required and thus could be erroneous[138]; and
- The Lockheed System does not track and manage Security Information as required, so Security Operators cannot rely on it to be up---to---date, comprehensive, and relevant in context to Emergency Response Plans[139]

289. Unreliable Security Information cannot be used with the speed and accuracy contractually mandated in the Required System. Consequently, more people may be killed or injured, more property may be damaged, and MTA operations may be interrupted for longer periods of time than would be the case if Security Operators could properly rely on Security Information as they would have been able to do had Lockheed satisfied these requirements.

C.3. Lack of Understanding of Security Information

290. With regard to the subset of Admitted Non---Passed Requirements analyzed in

[138] RQMT 2281.1 ("The Contractor shall provide a Command and Control System where all user--- entered data is validated for reasonableness of content"); RQMT 2056 ("The Contractor shall provide all asset and resource information that identifies the source of the information"); RQMT 2281.4 ("The Contractor shall provide a Command and Control System where all user---entered data is validated for reasonableness of content"); RQMT 2282.1 ("The Contractor shall provide a Command and Control System where data validations include intra---field and inter---field validations"); RQMT 2282.3; ("The Contractor shall provide a Command and Control System where data validations include intra---field and inter---field validations"); RQMT 2282.4 ("The Contractor shall provide a Command and Control System where data validations include intra---field and inter---field validations"); RQMT 2205 ("The Contractor shall provide a Command and Control System that is capable of displaying alarm information; obtained from field devices such as electronic detectors/sensors, cameras, access controls and intrusion devices").

[139] RQMT 1978 ("The Contractor shall provide a system that maintains a historical log of all changes to the Response Plan"); RQMT 2033 ("The Contractor shall collect information from the Response Plan and task execution times, and who provided portions of the plan"); RQMT 2034 ("The Contractor shall collect information on the applicability of the Response Plan (e.g., number of changes made to the plan) and by whom").

this section, the Lockheed System creates situations in which a Security Operator cannot understand Security Information (and would be better able to understand Security Information under the Required System) because:

- The Lockheed System does not provide required training functions to prepare Security Operators to best learn how to operate and practice using the system[140];

- The Lockheed System does not provide sufficient information about the source of Security Information[141]; and

[140] RQMT 2871 (“The Contractor shall ensure authorized C2 Users are able to log onto the system, at workstations allocated for training/testing, using the same log on displays and accesses (username and password) used for normal operations”); RQMT 2872 (“The Contractor shall ensure authorized C2 Users inherit access rights based upon their user classification (Instructor, Trainee, and Tester”)); RQMT 2878 (“The Contractor shall provide a Simulator that supports the simulation of all conditions and functions supported by the IESS”); RQMT 2884 (“The Contractor shall provide a Simulator that simulates the normal and failure operation of the security devices within the system by using programmed simulation data and/or simulated external inputs”); RQMT 2885 (“The Contractor shall provide a Simulator that emulates responses to the data, controls and messages produced by the Command and Control System, such that, data exchanged between the simulator and the Command and Control System matches the unprocessed data exchanged between the Command and Control System and the security devices in content, format and timing”); RQMT 2886 (“The Contractor shall provide a Simulator that simulates the operation and functionality of any external device or system by using data previously received from the Command and Control System (e.g., video streams), data generated as part of the simulation”); RQMT 2887 (“The Contractor shall provide a Simulator that is capable of generating simulated data for all possible commanded and uncommanded changes of state for all devices”); RQMT 2888 (“The Contractor shall provide a Simulator that is capable of generating simulated data for all controls, indications and alarms for all external devices”); RQMT 2889 (“The Contractor shall provide a Simulator that is capable of generating simulated data for all external systems”); RQMT 2890 (“The Contractor shall provide a Simulator that is capable of generating simulated data for both normal and error responses to data received from the Command and Control System, data generated by the simulation scenario, and manual inputs from an authorized”); RQMT 2902 (“The Contractor shall provide simulation data to be retrieved that includes the appropriate versions of system databases, software versions, and control data to form a complete and accurate version of the Command and Control System for the requested simulation time period”); RQMT 2906 (“The Contractor shall provide a simulation system that provides the ability to select and connect to the voice communication channels for a Trainee”); RQMT 2907 (“The Contractor shall provide simulation software that provides the ability to record and playback the IESS responses and results that would arise on the real---time IESS as a consequence of the trainee's actions”); RQMT 2916 (“The Contractor shall design the Simulator so that it can be updated for modifications of devices that exist in the system”); RQMT 2918 (“The Contractor shall design the Simulator so that it can be updated for modifications to the system to add new devices or device types”); RQMT 2919 (“The Contractor shall design the Simulator so that it can be updated for modifications to external systems”); RQMT 2929 (“The Contractor shall provide simulation scenarios to control the behavior of the simulation by injecting or overriding inputs and outputs to simulate a specific condition”); RQMT 2930 (“The Contractor shall provide Scenario Creation Displays that allows users to create, modify and delete simulation scenarios”); RQMT 2932 (“The Contractor shall provide Scenario Creation Displays that allows users to populate a simulation scenario with historical archival data that has been stored on an archive medium”); RQMT 2933 (“The Contractor shall ensure users are capable of starting a simulation session and storing all system activity for that simulation session into a simulation scenario log”).

[141] RQMT 2115.2 (“The Contractor shall provide a Command and Control System that logs all alarm analysis information, including raw data used to determine the alarm (I---Alarm)”); RQMT 2450 (“The Contractor shall

- The Lockheed System does not deliver automated decision support tools as required.[142]

291. Security Operators cannot use Security Information that is not properly understood with the speed and accuracy mandated by the Contract requirements. Consequently, more people may be killed or injured, more property may be damaged, and MTA operations may be interrupted for longer periods of time than if Security Operators had the contractually mandated tools to properly understand Security Information.

C.4. Inability to Manage and Communicate Security Information

292. With regard to the subset of Admitted Non---Passed Requirements analyzed in this section, the Lockheed System creates situations in which a Security Operator cannot manage and communicate Security Information (and would be better able to do so under the Required System) because:

- The Lockheed System does not help Security Operators prioritize actions as required[143];
- The Lockheed System lacks required tools to manage Security Information both during and after a Security Event[144]; and

ensure data automatically entered by Alarm Management includes, but is not limited to date, time, a marker indicating whether the operational event has been automatically or manually generated, person entering the event, the alarm that precipitated the automatic creation of the event, the location involved in the event, and a serialized operational event number"); RQMT 2590 ("The Contractor shall ensure data on the alarm display(s) includes the alarm's system source").

[142] RQMT 1850 ("The Contractor shall provide a system, which funnels Alerts/Alarms upwards according to the business rules and the Decision Support Subsystem"); RQMT 1910 ("The Contractor shall ensure that a message is generated and published on the message bus when a security event (e.g., Incident or Emergency Situation) occurs, based upon the business rules"); RQMT 1912 ("The Contractor shall provide Incident Management/Decision Support that is automatically initiated once a security event message is received, based upon the appropriate business rules for the C3 Center"). See also RQMTs 8, 1846, 2047, 1899, 1851, 1912, 1925, 1936, 1937, 1938, 1941, 1942, 1950, 1962, 1964, 1989, 2047.2, 2048, 2116, 2280, 2539, 2915, 3010, 3016, 17050 and 17060.

[143] RQMT 2138 ("The Contractor shall provide a Command and Control System that provides for rapid evaluation of available information to quickly determine situations requiring attention (e.g., emergencies, terrorist attacks, and life threatening incidents")); RQMT 3013 ("The Contractor shall ensure the System Administrator has the ability to add, delete or edit the criticality/priority of the tasks (e.g., if the same task supports multiple strategies, then this task is a higher priority, saving lives is more critical for assigning resources"));RQMT 2620 ("The Contractor shall provide Alarm Management that provides the functionality to allow authorized C2 Users to enter/modify the alarm, alert or notification messages, text and any attributes").

- The Lockheed System does not allow certain communications of Security Information as required.[145]

293. Due to the above-described failings in the Lockheed System, Security Operators cannot manage and communicate Security Information with the speed and accuracy required. Consequently, more people may be killed or injured, more property may be damaged, and MTA operations may be interrupted for longer periods of time than if Security Operators could manage and communicate Security Information as mandated by the Required System.

C.5. System Inflexibility

294. With regard to the subset of Admitted Non-Passed Requirements analyzed in this

[144] RQMT 2798 ("The Contractor shall provide a Command and Control System that allows authorized C2 Users to call up any display or request any report, including opening those which may not have been presented at the time of the recording of the events"); RQMT 2800 ("The Contractor shall provide a Collaboration capability that provides integrated voice, video, graphics, data and white--- boarding functions"); RQMT 3096.2 ("The Contractor shall provide a Security Audit capability that generates an alarm to the authorized administrator if the audit trail exceeds the administrator--- specified log size defaulted to two days"); RQMT 3151 ("The Contractor shall provide Access Management with an on---line mechanism that provides for a real---time update of all C3 Center computer system users currently logged in, along with the locations and workstations that they are logged into"); RQMT 3155 ("The Contractor shall ensure the data includes the C3 Center Computer system user who performed or attempted the function"); RQMT 3156 ("The Contractor shall provide Access Management that provides an audit trail for tracking system management activities such as modifying system parameters and creating, editing, or deleting user accounts with regard to login information"); RQMT 3182 ("The Contractor shall provide territories that can be aligned, or realigned, by an authorized C3 User utilizing an on---line configuration editing function, provided as part of Access Management"); RQMT 3188 ("The Contractor shall provide Access Management that issues an alarm if changing territory selections for a user will leave a section(s) of territory unmonitored"); RQMT 2104 ("The Contractor shall provide Monitor and Control Sensors that evaluates network information and provides the authorized C2 User the ability to reconfigure the network when a communication situation/problem occurs").

[145] RQMT 2047.1 ("The Contractor shall provide device controllers that create, aggregate and forward alarm indicators based upon pre---defined business rules and access control"); RQMT 2468 ("The Contractor shall provide a system that allows authorized C2 Users to specify that a failure notification be logged, sent as an e---mail message to a user specified distribution list, or both"); RQMT 2470 ("The Contractor shall provide Failure Notifications that include errors that occur during distribution of messages"); RQMT 2527 ("All alarms from separate subsystems, such as an equipment room intrusion, a suspicious package detected by the intelligent CCTV system, or a denial of service attack indicated by a router managed by a NMS, shall be integrated into Alarm Management capability"); RQMT 2578 ("The Contractor shall provide Alarm Management that logs Alarms, Alerts and Notifications, even if they are inhibited"); RQMT 2611.2 ("The Contractor shall ensure any and all additions and/or modifications to the set of defined Alarms, Alerts or Notifications shall be logged to a database"); RQMT 2944.2 ("The Contractor shall provide an Employee Information function that provides an authorized C2 User the ability to locate an Employee's on---line information based upon entry of their name (whole or partial) or their employee number (Additional C3)"); RQMT 2969 ("The Contractor shall ensure an authorized C2 User is required to specify default distribution lists ('To' list, 'From' list, 'cc' list or conventional mail list") for all automatically generated reports"); RQMT 3665 ("The Contractor shall provide the hardware and software necessary to allow the VCS to send and receive FAX messages").

section, the Lockheed System creates situations in which Security Operators cannot enter and interact with Security Information in a flexible manner because:

- The Lockheed System does not allow for the individual adjustment of the frame rate, resolution, and bandwidth for each camera in the system as required;[146]
- The Lockheed System does not support portable devices as required;[147]
- Security Operators cannot reconfigure the network as required when a communication situation or problem occurs;[148] and
- Security Operators cannot update Emergency Response Plans or the Training Simulator Module as required.[149]

295. Because of this lack of flexibility – considered both independently and in conjunction with the Lockheed System's significant gaps in functionality – Security Operators are more likely to miss, are less able to rely upon, and are less likely to understand and effectively manage and/or communicate Security Information than would be the case had Lockheed satisfied these requirements. Consequently, more people may be killed or injured, more property may be damaged, and MTA operations may be interrupted for longer periods of

[146] RQMT 14783 ("The frame rate, resolution and bandwidth for each camera shall be individually adjustable").

[147] RQMT 2158 ("The Contractor shall provide a Common Operational Picture that supports displays on portable devices of different form factors (notebook computers, cell phones, PDAs)"); RQMT 2159 ("The Contractor shall provide a Command and Control System that allows the users of these portable devices to customize their display/output selections"); RQMT 2309 ("The Contractor shall present on displays at each Local C3 Center, status information for each device, under the jurisdiction of that Local C3 Center"); RQMT 2310 ("The Contractor shall present on displays at each Regional C3 Center, status information for each device, under the jurisdiction of that Regional C3 Center and for the devices of each Local C3 Center that is under the jurisdiction of that Regional C3 Center"); RQMT 2862 ("The Contractor shall provide an Emergency Tracking Site that is web---based, disseminating nearly up to date information to authorized personnel with remote computer access, through Internet accessible PDA or cell phones").

[148] RQMT 2104 ("The Contractor shall provide Monitor and Control Sensors that evaluates network information and provides the authorized C2 User the ability to reconfigure the network when a communication situation/problem occurs").

[149] RQMT 1978 ("The Contractor shall provide a system that maintains a historical log of all changes to the Response Plan"); RQMT 2916 ("The Contractor shall design the Simulator so that it can be updated for modifications of devices that exist in the system"); RQMT 2918 ("The Contractor shall design the Simulator so that it can be updated for modifications to the system to add new devices or device types"); RQMT 2919 ("The Contractor shall design the Simulator so that it can be updated for modifications to external systems").

time than if Security Operators were able to flexibly interact with the System as called for by the Required System.

C.6. Insecure Security Information

296. With regard to the subset of Admitted Non---Passed Requirements analyzed in this section, the Lockheed System creates situations in which Security Information is less secure than required under the Required System because:

- The Lockheed System leaves sensitive data more open and vulnerable to attack than the Required System[150]; and

- The Lockheed System makes it more difficult or impossible to tell that data has been compromised compared to the Required System.[151]

297. Because of this lack of IT security in the Lockheed System, the entire IESS/C3 SoS is more vulnerable to penetration and consequent shutdown, denial of service, and compromise of sensitive data than it would have been had Lockheed satisfied these requirements.

C.7. Inefficiency

298. With regard to the subset of Admitted Non-Passed Requirements analyzed in this section, the Lockheed System is more cumbersome to operate than the Required System because:

- The Lockheed System requires Security Operators to manually look up information in a cumbersome manner, which would not have been the case had Lockheed satisfied these requirements[152]; and

[150] RQMT 3062 ("The Contractor shall provide security to ensure that the Data Access Log cannot be modified or deleted by the C2 Users and only the System Administrator can delete a Data Access Log."); RQMT 3103 ("The Contractor shall provide virus protection software that is current and operational at all times on all system processors.").

[151] RQMT 3292 ("Database security shall be provided to trace all user accesses/attempts and all attempts, entries and updates to the database via audit logs"), RQMT 3096.2 ("The Contractor shall provide a Security Audit capability that generates an alarm to the authorized administrator if the audit trail exceeds the administrator---specified log size defaulted to two days").

[152] RQMT 2056 ("The Contractor shall provide all asset and resource information that identifies the source of the information"); RQMT 2205 ("The Contractor shall provide a Command and Control System that is capable of displaying alarm information; obtained from field devices such as electronic detectors/sensors, cameras, access

- The Lockheed System does not provide function keys for quick access to critical functions.[153]

299. Because the Lockheed System is more cumbersome to operate than would be the case under the Required System. The cumbersome nature of the Lockheed System, combined with its underlying lack of functionality compared to the Required System, means that Security Operators will use it less efficiently and effectively than would have been the case under the Required System.

C.8. Summary of Consequences of Admitted Non-Passed Requirements

300. An analysis of the Admitted Non-Passed Requirements – both independently (in this response to the Aella/DeStefano Report) and in conjunction with the overall system shortcomings as reflected in the project testing record and examined in my Initial Expert Report – reveals that the Lockheed System is significantly less effective than the Required System. Consequently, MTA's customers, employees, facilities and operations are at greater risk, and its security operations are less efficient than would be the case if Lockheed delivered the Required System.

V. Additional Response to Aella/DeStefano Report's Assertions Regarding Lockheed's Performance on Project C--52038

A. Overview of the Aella/DeStefano Report's Assertions of Lockheed's Performance compared to Lockheed's Actual Performance

301. In its RFP response, Lockheed agreed to meet 100% of the requirements of Project C-52038.[154] Lockheed represented that it was able to meet the project's technical

controls and intrusion devices"); RQMT 2450 ("The Contractor shall ensure data automatically entered by Alarm Management includes, but is not limited to date, time, a marker indicating whether the operational event has been automatically or manually generated, person entering the event, the alarm that precipitated the automatic creation of the event, the location involved in the event, and a serialized operational event number").

[153] RQMT 2291.3 ("The Contractor shall program function keys for quick access to critical, key functions").

[154] See Footnote 13 above.

requirements based on its carefully considered technical solution,[155] its highly--- qualified staff,[156] and a project management plan that adhered to the highest standards of effectiveness and efficiency.[157]

302. The Aella/DeStefano Report opines that Lockheed proposed a proper solution, appropriately responded to the RFP, and effectively staffed, managed, and implemented the project until termination.[158] It further opines that "if Lockheed Martin had not been terminated, the project would have been successfully completed and the [MTA] agencies would be fully utilizing the system."[159]

303. Based on my examination of the project records, my communications with MTA staff, contractors and experts,[160] my understanding of the "bottom line" results of the myriad testing failures, and my personal on-site observations of what the MTA has managed to develop and use from the system that Lockheed left when it was terminated, I have concluded that Lockheed did not properly design, procure, staff, or deliver the Required System.

[155] See Lockheed Martin Proposal, Volume 2, 3.1 Design Development, Solicitation No. C---52038, July 22, 2005, at 80 ("This process provides a starting point that has been carefully considered and designed to meet the specified requirements. A design that has a solid basis will facilitate any necessary open---forum discussions to clearly understand customer requests and requirements concerns.").

[156] See Lockheed Martin Proposal, Volume 3, 2.1 Key Personnel, Solicitation No. C---52038, July 22, 2005, at 6 ("Because the IESS/C3 project is so critical, we have chosen to designate all of our principal staff members as key personnel. This will ensure the availability of this staff immediately upon contract award and their continued availability throughout the program. The assignment of these highly qualified individuals to the project is a clear demonstration of our Team's respective corporate commitments to the program.").

[157] See Lockheed Martin Proposal, Volume III, 1.0 Introduction, Solicitation No. C---52038, July 22, 2005, at 1 ("The Lockheed Martin/ARINC Team provides an industry best practice Program Management structure that encompasses all program elements to deliver true program performance.").

[158] See Aella/DeStefano Report at 2.

[159] Aella/DeStefano Report at 97.

[160] Such individuals include Joseph Christen (MTACC), Ronald Pezik (MTACC), Kenneth Shields (URS), Terrence Fetters (Parsons), Shirish Gupte (Parsons), William Morange (MTAPD), Ronald Masciana (MTAPD), Ernest Pucillo (MTAPD), William Coan (MTAPD), Ray McDermott (MTAPD), Leonard Viviano (MTAPD), Robert Murphy (LIRR), John Hyland, (LIRR), Sean Ryan (MNR), April Panzer (MNR), Lisa Schreibman (NYCT), Howard Reith (Dnutch) and staff at GuidePost Solutions (Adam Safir, Chris Grajcar and Ron Chandler).

304. Because it is not productive, this declaration does not detail the immense and palpable dissatisfaction of MTA employees and contractors with Lockheed's project management actions and omissions that resulted in the shortcomings of the Lockheed System. I do believe, however, that responding to several arguments asserted in the Aella/DeStefano Report that incorporate such actions and omissions on the part of Lockheed will help further illustrate why such dissatisfaction exists and why I believe that, without a significant change in how it conducted business, Lockheed would not have delivered the Required System, even if it had been given more time and money to do so.

B. Lockheed Did Not Deliver the Level of Security Expertise Required to Guide and Inform Project C-52038

305. The Aella / DeStefano Report claims that "Lockheed Martin appropriately staffed the project, managed the challenges and changes for this type of project and was progressing work as expediently as the project conditions allowed."[161] Based on the testing records and my conversations with MTA employees, I disagree with the Aella/DeStefano Report's conclusion.

306. As a first example, Lockheed contributed very little to the Concept of Operations (CONOPS), a critical document that Lockheed was contractually required to deliver to set forth its strategic vision and certain details of how the system was to be used. The fact that Lockheed did not make any substantive changes to the draft CONOPS whatsoever — the document remaining virtually unchanged from the draft document developed by Parsons that was available to Lockheed at the beginning of the project[162] — indicates to me that Lockheed paid little attention to and/or greatly discounted this important document, and with it the fact that the

[161] Aella / DeStefano Report at 2.

[162] See Requirement 34 , ("A detailed Concept of Operations (ConOps) shall also be developed as a part of this effort with Agency---specific ConOps."); see also Requirements 3304, 3308, 3312 and 3317.

security system would be used by security operators as part of an overall security strategy. Furthermore, Lockheed's failure to provide any substantive advancement to the CONOPS was in stark contrast to what they represented in their RFP Response:

> "The overall SoS ConOps included as reference material in Volume 6A of the RFP will be used as guidance for creating a baseline IESS/C3 overall ConOps updated with scenarios added and its evolution progressed in step with the development of Agency---specific ConOps. The National Incident Management System (NIMS) ConOps will also provide guidance to development of these ConOps. The ConOps for MTA and its agencies will comply with the recommendations of IEEE Std 1362---1998, IEEE Guide for Information Technology – System Definition – Concept of Operations Document.
> Lockheed Martin/ARINC Team members have previously developed an IEEE---compliant ConOps for NYCT's ATS---B system."[163]

307. As a second example, Lockheed's lack of appropriately coherent, methodical, and comprehensive consideration of the impact of the IESS/C3 SoS on security operations is further evidenced by the disjointed and incomplete nature by which Lockheed developed (or did not develop) business rules, use cases and training materials.[164] In fact, Parsons developed plain English business rules, again without substantive input from Lockheed.[165] In the case of Intra---agency Business Rules, Lockheed reduced what Parsons drafted to "If---Then---Else" statements for the system level, again with very little substantive input to the creation of the business rules themselves.[166] In the case of Interagency Business Rules, Lockheed did not meaningfully participate in their development or accept the ones that were presented by Parsons by the Date of Termination.[167]

[163] Lockheed Proposal, Volume II, Page 87

[164] See email from Shirish Gupte to Ron Pezik of October 2, 2008 regarding the status of the Business Rules (MTACC_E 0000499434).

[165] Id.

[166] Id.

[167] Id.

308. Because the business rules were essentially the "brains" behind what was supposed to be a "smart" system, Lockheed's unwillingness or inability to take a leadership role in their development further indicates to me that Lockheed did not approach, manage or deliver this project as required.

C. The Lockheed System as Evidenced by the Lockheed Expert Site Inspection

309. Contrary to the inaccurate arguments in Section VII of the Aella/DeStefano Report that include out-of-context quotes of MTA employees,[168] and notable omissions of what Lockheed Representatives[169] saw and heard when they visited various MTA sites on March 22 and March 23, 2011,[170] huge overall gaps in functionality and many specific limitations of the Lockheed System were clearly demonstrated and/or orally communicated to Lockheed Representatives at those site visits. In addition, MTA representatives explicitly told Lockheed Representatives that certain required elements were not functioning at all or as required at the time of Default.[171]

[168] For example, the statement in the Aella/DeStefano Report at 98 that "MTA MNR employee April Panzer said that her department was able go---live with the system at MNR on their own using Lockheed Martin provided equipment which had been in storage" is wholly misleading since the term "go live" has no bearing whatsoever on whether the system that is to "go live" is the system specified by the Contract. I understood Ms. Panzer's statement to mean that MNR has a system that does not even closely approximate project requirements, but that they can use for some limited functionality. Likewise, the Aella/DeStefano Report's characterization of Robert Murphy's issues with i/Consequence as a "misconception" regarding integration with i/Asset does not give the proper context,. As explained by Mr. Murphy, i/Consequence does not meet the technical requirements of the Contract and he found i/Consequence on its own to be wholly inadequate for use.

[169] Lockheed Representatives included Gregory Bernardo of Aella Consulting Group, Louis T. DeStefano and Abe DeStefano of Louis T. DeStefano, Inc., Michael Chartan, Sandra Jeskie, Matthew Taylor, Brian Markowitz and Nicole Woolard of Duane Morris law firm, and John Steinbock and Mark Smith of Lockheed Martin. Representatives of the Surety Company included Adam Friedman (Day one only) and Brian Kantar (Day two only).

[170] Sites visited by Lockheed Representatives included the site for the Central C3 Center (MTAPD Headquarters in Long Island City), for the LIRR C3 Center (Jamaica Control Complex), the Server Room at 341/10 Madison Avenue, the Metro North Railroad C3 Center (North White Plains), Metro North terminals at the Grand Central Terminal Refrigeration Plant, the GCT 7th Floor Situation Room, and the NYCT C3 Center on Livingston Street in Brooklyn.

171 At the Central C3 Center (March 22nd) MTA Representatives Shirish Gupte and Len Viviano communicated to Lockheed Representatives that certain aspects of the Lockheed System were not functioning as required at the time of Default, namely:

i) critical decision making (i/Consequence) and system management (i/Asset) tools had only been installed at LIRR, had limited data and that LIRR was "making an attempt" to use it;

ii) Lockheed provided no operator training or the required "training scenarios", resulting in operators needing to train on a live system;

iii) NetMotion was not being used;

iv) the only video analytics in use at all was "Tripwire";

v) the system lacked the ability to control access from the Central C3 Center; vi) operators had no control over events but were "just monitoring";

vii) the Activu Screen display system had difficulty automatically discovering cameras, and experienced delays in camera feeds and issues getting the camera feeds to properly fit on the screen;

viii) the retrieval of video clips were not functioning based on existing policy;

ix) only a "limited subset" of the system to monitor and manage the functionality of devices (HPOpenView) could be used; x) externally---recorded events were not functioning to populate a database; xi) the feature for determining whether a camera was not working was "not functional" other than through a subsystem (Broadware);

xii) Zetron was identified as a "completely separate" system with no interfaces to databases, indicting a failure of integration; and

xiii) the ability of Software (NICE---Inform) to create and thus manage multiple incidents was explained as being implemented entirely post---default.

At the Jamaica Control Complex (March 22nd), it was communicated to Lockheed Representatives that certain aspects of the Lockheed System were not functioning as required at the time of Default, namely:

i) there was no Single---Sign on Password System;

ii) LIRR could not use/Asset (and Lockheed engineers expressed to LIRR that it was of no value);

iii) Lockheed did not deliver "Shared space" (i.e. shared folders)

iv) the infrared cameras supplied by Lockheed did not function;

iv) i/Consequence was described as "completely manual" (CAD events did not come in automatically and they "go nowhere"; choices given to the operator were "in no way interactive" and differentiation of data from different events was supposed to be based on geocoding (i.e. "LIRR land" versus "Amtrak Land") but "this does not work either");

v) much of the functionality of Intergraph that "wasn't there" at the time of Default was still "not there at the time of inspection";

vi) the CAD System was not mapping correctly;

vii) there was no alarm logging;

viii) Lockheed did not provide a single contact directory as required, but instead provided two directories;

ix) Lockheed did not provide any training manuals;

x) in some locations, Lockheed provided indoor cameras not suitable for outdoor use;

xi) the audio recovery capability of NICE was never made functional;

xii) Lockheed's geo---mapping incorrectly reported cameras to be over train tracks;

xiii) cameras and alarms were not correlated as required; and

xiv) alarms and GIS were not correlated as required.

At the Server Room at 341/10 Madison Ave (March 22nd), it was shown to Lockheed Representatives at this time and location that:

i) this was supposed to be a backup room for the Required System, but it was never set up as such;

ii) there is no HP OpenView at this location; and

iii) the Cisco equipment here was installed by Lockheed but may have to be repurposed to work somewhere else.

At the Metro North Railroad C3 Center in North White Plains (March 23rd), it was communicated to Lockheed Representatives that certain aspects of the Lockheed System were not functioning as required the time of Default, namely:

i) the functionality of this facility was limited to the monitoring of cameras;

ii) NICE Audio was not functional;

iii) Zetron was not functional;

iv) nothing could trigger an alarm at a Metro---North facility;

v) some of the color cameras were displaying in black and white;

vi) the ability to create an "event" was not operational;

vii) recording of cameras overwrites every 24 hours and did not meet the 30 day storage requirement of the Required System;

viii) there was no Intergraph training;

xix) there was no differentiation between floors and limited detail representing cameras on geospatial maps; ix) sometimes cameras got "stuck";

x) to see a video clip, an operator needed to login to a separate subsystem (Broadware);

xi) there were latency issues with "multiple cameras that have a lot of activity";

xii) there was a spinning, malfunctioning Pan---Tilt---Zoom Camera that was acknowledged by Gregory Bernardo of Aella Consulting to be "possessed"; and

xiii) the security operator did not know how to playback stored video.

Len Viviano, the head of MTAPD IT was able to playback stored video, but the playback was "jumpy" and did "not speed up properly" (and the same problems existed at Long Island City). At the Central Terminal Refrigeration Plant (March 23rd), it was shown or communicated to Lockheed Representatives that:

i) the operator workstation did not boot;

ii) the administrator workstation had limited software installed on it that did not load properly; and

iii) user IDs were not segmented properly.

At the Grand Central Terminal ("GCT") 7th Floor Situation Room (March 23rd), it was shown or communicated to Lockheed Representatives at this time and location that:

i) the same limited functionality as the MNR C3 center visited earlier in North White Plains exists at GCT (i.e. only looking at cameras and not monitoring alarms) but without the Activu monitors;

ii) the 7th Floor Situation room and the North White Plains facility visited earlier represent two of the four local C3 centers envisioned and that the other two (District 5 HQ of MTAPD and the Fire Command Center) do not have any equipment installed;

iii) Single---Sign On had not been implemented and did not work;

iv) device maps had limited details;

v) cameras had similar video quality issues to the MNR C3 center; and

vi) tower and screens were delivered by LM, but MTA may have done additional work after default to make them operational.

At the NYCT C3 Center (March 23rd), it was shown or communicated to Lockheed Representatives that:

i) the system that Lockheed worked on was not operational at all;

ii) NYCT cameras were monitored by a separate system run by the NYPD because NYPD felt compelled to "step in" when the Required System was not functional;

iii) the extent to which cameras would be monitored by the NYCT C3 Center when "made functional" was "still being worked out";

iv) NYPD gave MTA "limited access" to the cameras and MTA had "very little control" (i.e. could not archive or playback));

v) Lockheed mounted cameras but did not necessarily connect them ;

vi) no Access Control system data was coming into the center (Lenel);

vii) the Activu video wall installed by Lockheed was six inches too low, so that if operators ever used it, those in the back row would not be able to see it (the group observed the a modular solution was implemented to raise the wall);

viii) Zetron was installed but was not functional;

310. In addition to Lockheed's failures to pass myriad technical requirements as shown through the project testing record, the shortcomings shown and communicated to Lockheed Representatives at the site visits demonstrated that the Lockheed System they were witnessing, even where it had been made minimally operational by MTA's own efforts, still did not provide Security Operators the tools or training to be adequately aware of, or to be able to rely upon, manage, communicate, or secure Security Information; and further, that the Lockheed System they were witnessing, even where it had been made minimally operational by MTA's efforts was cumbersome to operate.

311. At many instances during the site visits, the Lockheed Representatives' primary questioner — Gregory Bernard of Aella Consulting Group— acknowledged the limited functionality and overly manual nature of the Lockheed System. For example:

- While discussing the Central C3 Center at Long Island City, Mr. Bernardo remarked "this is all reactionary and investigations." In the security industry, it is widely understood that a "reactionary" system that is good only for "investigations" is a substandard system that will not provide the ability to prevent security incidents. The Required System was clearly not intended to be "reactionary."

- During a discussion of the geocoding issues at the LIRR C3 Center, Mr. Bernardo remarked, "So it's definitely not functioning, right? Obviously."

- While observing the limited function of camera monitoring at the MNR C3 Center at White Plains, Mr. Bernardo said, "so we're really looking at the full functionality here," indicating that he understood that the "full functionality" that MNR has now is nowhere near the "full functionality" that MNR was supposed to receive.

ix) the center had no capability of responding to security events;

x) there was a legacy Lenel access control system that was not connected to the camera monitoring system;

xi) there was no single---sign on capability; and

xii) for the planned backup centers at the Bus Command Center, Presidents Conference Room, and Staten Island, equipment had been delivered but "no work was done."

- When Mr. Bernardo observed the jumpy playback of archive video at the MNR C3 center he remarked "this does not meet a VCR---like expectation," and he simply said "wow" when he was shown how difficult it was to get archive video.

- While observing the NYCT C3 Center's inability to monitor alarms, Mr. Bernardo compared the NYCT C3 center to a "stepchild" and noted that it was "isolated."

312. The arguments in the Aella/DeStefano Report that the MTA did not receive a "system integrator value add"[172] after Lockheed was terminated (presumably to meet project requirements where Lockheed failed to do so), did not "have a complete understanding of the how the various subsystems were designed to be interfaced,"[173] and "relaxed" requirements since termination[174] amount to little more than irrelevant criticism of the MTA's post---default attempts to salvage operational usefulness from the Lockheed System, and further highlight the operational and financial damage Lockheed caused to the MTA.

VI. Conclusion

313. It is my expert opinion, based on the Project records and my observations, that i) Lockheed failed to pass a large number of critical and important technical requirements, ii) Lockheed failed to integrate various subsystems into the Required System, and iii) Lockheed failed to develop of relevant, effective security operations documentation and training as to how the system would function and be used by Security Operators to protect MTA Assets.

314. Against this backdrop, the Aella/DeStefano Report essentially argues that Lockheed did not have to meet contractual requirements because the products that Lockheed chose to meet the requirements could not do what the MTA required, all while trying to "blame the victim" for various complexities in procurement and program management for a program that

[172] Aella/DeStefano Report at 98.

[173] Aella/DeStefano Report at 100.

[174] Aella/DeStefano Report at 98.

Lockheed represented that it was qualified and capable of properly managing.

315. In my view, this argument boils down to a contention that Lockheed's role in Project C---52038 was no more than that of a local alarm dealer installing an off---the---shelf security system in a local store, without accounting for the intricacies of the particular building or business.

316. As explained in this declaration, what the MTA received from Lockheed was not even close to "good enough" compared to what was required by the Contract. The consequences of Lockheed's failure to deliver the Required System are highly significant and potentially tragic.

Howard Safir

Exhibit A

Resume of Howard Safir

I have held various positions of authority and responsibility for leading law enforcement and emergency management organizations, including service as the 39th Police Commissioner of the New York City Police Department (1996-2000), the 29th Fire Commissioner of the New York City Fire Department (1994-1996), Associate Director for Operations of the United States Marshals Service (1984 - 1990), Director of the Federal Witness Security Program (1979 - 1984), and various roles with the Drug Enforcement Administration (1965 - 1979, including predecessor agencies FBN and BNDD).

Since retiring from government service in 2000, I have worked as a security and risk mitigation consultant (from 2001 until April, 2010 as Chairman and CEO of SafirRosetti; from April, 2010 to the present day as Chairman and CEO of Vigilant Resources International (VRI)). Additional relevant private sector work I have performed includes acting as Special Advisor to the Chairman of ChoicePoint (2000-2005), and active roles as a Board member for Verint Technologies, Lexis Nexis Special Solutions and Implant Sciences Corporation.
My experience relevant to how electronic security and emergency management systems are most effectively implemented and utilized includes, but is not limited to, the following:

- As Police Commissioner I was ultimately responsible for the protocols, procedures and actions pertaining to how sworn officers interacted with various electronic security and emergency management systems to successfully fulfill their mission. These systems included the 911 Center which included dispatch and call intake for over a million calls a year for assistance in emergency situations, the closed-circuit TV systems that were installed in many of the public housing devlepments in NYC, and the NYPD radio system that communicated between our 6,000 vehicles, 26 boats and 7 helicopters.

- As chief of operations of the US Marshals service I was responsible for the CCTV systems, perimeter alarms, radio systems And access control systems for the 76 federal judicial districts, and the several hundred facilities in those districts including the witness security facilities throughout the nation.

- As Fire Commissioner I was ultimately responsible for the protocols, procedures and actions pertaining to how FDNY responders interacted with various electronic emergency management systems to successfully fulfill their mission. These systems included the six emergency dispatch centers and the CAD system that connected them, the radio system that connected the 276 fire houses and their vehicles and the EMS computer system and radio system.

- As CEO of SafirRosetti and VRI, I have been ultimately responsible for the services that these companies have provided to assess threats, risks and vulnerabilities, implement electronic security and emergency management systems, and draft, implement and train operators to carry out effective security and emergency management policies and procedures. Clients with significant facilities and operations in New York City where I have overseen the implementation of *policies. procedures and programs regarding how to most effectivelv operate* electronic security and emergency management systems and have ultimately been responsible *for the design and implementation of capital improvements to securitv and emergencv management svstems* include KeySpan (now National Grid), the New York Yankees (New Yankee Stadium), and the New York Jets/Giants (New Meadowlands Stadium).

As an active Board member of Verint Systems, LexisNexis Special Solutions and Implant Sciences, I have additional exposure to further understand how effective management of data, information and intelligence may support the operation of electronic security and emergency management systems by security and emergency responders.

I have not testified as an expert witness in the last four years. Prior to that period I testified as an expert witness regarding the emergency response to the September 11th attacks as part of the litigation between the World Trade Center's developer/owner and insurance companies.

Exhibit A

Resume of Howard Safir

I have held various positions of authority and responsibility for leading law enforcement and emergency management organizations, including service as the 39th Police Commissioner of the New York City Police Department (1996-2000), the 29th Fire Commissioner of the New York City Fire Department (1994-1996), Associate Director for Operations of the United States Marshals Service (1984 – 1990), Director of the Federal Witness Security Program (1979 – 1984), and various roles with the Drug Enforcement Administration (1965 - 1979, including predecessor agencies FBN and BNDD).

Since retiring from government service in 2000, I have worked as a security and risk mitigation consultant (from 2001 until April, 2010 as Chairman and CEO of SafirRosetti; from April, 2010 to the present day as Chairman and CEO of Vigilant Resources International (VRI)). Additional relevant private sector work I have performed includes acting as Special Advisor to the Chairman of ChoicePoint (2000-2005), and active roles as a Board member for Verint Technologies, Lexis Nexis Special Solutions and Implant Sciences Corporation.

My experience relevant to how electronic security and emergency management systems are most effectively implemented and utilized includes, but is not limited to, the following:

- As Police Commissioner I was ultimately responsible for the protocols, procedures and actions pertaining to how sworn officers interacted with various electronic security and emergency management systems to successfully fulfill their mission. These systems included the 911 Center which included dispatch and call intake for over a million calls a year for assistance in emergency situations, the closed-circuit TV systems that were installed in many of the public housing devlepments in NYC, and the NYPD radio system that communicated between our 6,000 vehicles, 26 boats and 7 helicopters.

- As chief of operations of the US Marshals service I was responsible for the CCTV systems, perimeter alarms, radio systems And access control systems for the 76 federal judicial districts, and the several hundred facilities in those districts including the witness security facilities throughout the nation.

- As Fire Commissioner I was ultimately responsible for the protocols, procedures and actions pertaining to how FDNY responders interacted with various electronic emergency management systems to successfully fulfill their mission. These systems included the six emergency dispatch centers and the CAD system that connected them, the radio system that connected the 276 fire houses and their vehicles and the EMS computer system and radio system.

- As CEO of SafirRosetti and VRI, I have been ultimately responsible for the services that these companies have provided to assess threats, risks and vulnerabilities, implement electronic security and emergency management systems, and draft, implement and train operators to carry out effective security and emergency management policies and procedures.
  Clients with significant facilities and operations in New York City where I have overseen the implementation of *policies, procedures and programs regarding how to most effectively operate* electronic security and emergency management systems and have ultimately been responsible *for the design and implementation of capital improvements to security and emergency management systems* include KeySpan (now National Grid), the New York Yankees (New Yankee Stadium), and the New York Jets/Giants (New Meadowlands Stadium).

  As an active Board member of Verint Systems, LexisNexis Special Solutions and Implant Sciences, I have additional exposure to further understand how effective management of data, information and intelligence may support the operation of electronic security and emergency management systems by security and emergency responders.

I have not testified as an expert witness in the last four years. Prior to that period I testified as an expert witness regarding the emergency response to the September 11th attacks as part of the litigation between the World Trade Center's developer/owner and insurance companies.